A Deus, que me guia e ilumina. Aos meus pais, Everaldo e Helenita, pela confiança e carinho. Ao meu esposo Beto, pelo apoio e paciência. Aos meus irmãos, familiares e amigos que sempre torcem por mim. Por fim, mas não menos importante, dedico este livro a Jacques e a Peter, por todos os ensinamentos que me passaram.

Raquel Vigolvino Lopes

Dedico este livro a Ana Lúcia, minha luz.

Jacques Philippe Sauvé

Aos diversos pais e mães que tive na vida, pais dos meus melhores amigos de infância, e especialmente aos meus pais Pedro e Elza que, com paciência, dedicação e amor, souberam transmitir para mim e meus amigos, verdadeiros ensinamentos de vida: humildade, honestidade, perseverança e respeito aos semelhantes.

Pedro Sérgio Nicolletti

Prefácio

O termo "melhores práticas" vem sendo utilizado no mercado para designar práticas e processos de trabalho utilizados por empresas ou equipes que, reconhecidamente, sejam bem sucedidas nas tarefas que empreendem. Empregar este termo na área de gerência de redes de computadores significa descrever práticas e processos que auxiliem um time de gerência de redes a manter o bom funcionamento de uma rede.

Bons livros que descrevem protocolos e bases de informações de gerência são facilmente encontrados no mercado. Mas a literatura de gerência de redes ainda é pobre quando mudamos de paradigma e buscamos materiais que nos ensinem como, na prática, obter, combinar e interpretar dados de gerência com o objetivo de efetivamente gerenciar uma rede.

Apesar da palavra "melhor" estar sendo empregada no termo "melhores práticas", isto não significa que as idéias descritas sejam perfeitas e que qualquer outra forma de se obter um determinado resultado seja errada. Significa apenas que, no momento, chegou-se a um consenso – por pesquisas e experiências – de que esta é, até então, uma forma com a qual equipes bem sucedidas obtiveram sucesso para alcançar um certo objetivo.

Objetivos

Este livro foi escrito com o objetivo de ajudar os profissionais responsáveis por gerenciar redes de computadores a atingir um melhor desempenho em seu trabalho. As melhores práticas para a gerência de redes de computadores encontradas aqui vão ajudá-lo a detectar, diagnosticar e solucionar problemas numa rede de forma eficaz. Você também encontrará boas práticas de configuração que, quando seguidas, podem evitar ou diminuir a probabilidade de ocorrência de certos problemas.

Os objetivos deste livro são, portanto:

- definir uma metodologia geral para detecção, diagnóstico e resolução de problemas de redes;
- descrever, de forma organizada, problemas que podem ocorrer em uma rede, mostrando seus sintomas, sinais e como podem ser confirmados e solucionados;
- mostrar como obter e interpretar algumas informações de gerência, tais como taxa de erros e utilização, que chamamos neste livro de *sinais*.

AUDIÊNCIA

Este livro foi escrito principalmente para profissionais responsáveis pela operação e resolução de problemas apresentados por uma rede. Mas outras pessoas podem se beneficiar também de sua leitura:

- pessoas responsáveis por desenvolver aplicações de gerência de redes. Para estas pessoas os procedimentos podem ser úteis, pois eles explicam como obter determinadas informações de gerência e como utilizar ou analisar a informação para chegar a conclusões sobre o estado de saúde de uma rede;
- estudantes ou outros profissionais interessados em aprender mais sobre a prática da gerência de redes.

ORGANIZAÇÃO

PARTE I: FUNDAMENTOS E ABORDAGEM

A Parte I deste livro é formada pelos Capítulos 1 a 3. O primeiro capítulo consiste de uma introdução geral à gerência de redes, uma analogia entre a Gerência de Redes e a Medicina e a apresentação de uma organização típica de um time de gerência. No Capítulo 2 explicamos o que são e como estão organizados o catálogo de problemas, os índices invertidos e os procedimentos. Finalmente, no Capítulo 3, definimos uma metodologia geral para detecção, diagnóstico e resolução de problemas de rede.

PARTE II: O CATÁLOGO DE PROBLEMAS

Na Parte II, formada pelos Capítulos 4 a 8, encontram-se o catálogo de problemas e os índices invertidos. Cada um destes capítulos – excetuando-se o Capítulo 8, no qual são apresentados os índices invertidos – encontramos problemas de uma determinada camada do modelo de referência OSI[1]. No Capítulo 4, por exemplo, encontram-se os problemas da camada física.

PARTE III: PROCEDIMENTOS

Os Capítulos 9 a 12 formam a Parte III deste livro. Neles encontram-se os procedimentos. Cada procedimento ensina pelo menos uma forma de se obter uma determinada informação de gerência. Procedimentos são referenciados no catálogo de problemas.

PARTE IV: APÊNDICES

A parte IV encontra-se no CD que acompanha este livro. Nela encontram-se capítulos teóricos sobre diversos temas de redes, como por exemplo: “Entendendo Ethernet” e “Introdução a VLANs”.

COMO LER ESTE LIVRO

Se você já estiver bastante familiarizado com o tema Gerência de Redes, tem uma idéia de como essa atividade se assemelha à atividade de um médico e conhece a organização típica de um time de gerência de redes, você pode pular o Capítulo 1.

---

[1] O modelo OSI foi criado como primeiro passo para a padronização internacional dos protocolos usados nas várias camadas.

Recomendamos que o Capítulo 2 seja lido pois ele explica como o catálogo de problemas, os índices invertidos e os procedimentos estão organizados e por quê. A leitura do Capítulo 3 também é recomendada. Nele apresentamos uma metodologia geral de detecção e resolução de problemas e mostramos como o restante do livro pode ser usado em conjunto com esta metodologia para auxiliar o gerente a diagnosticar e solucionar os problemas apresentados pela rede.

Este livro pode ser usado como um manual de primeiros socorros. Após levantar informações sobre um problema que está ocorrendo na rede no momento, veja no índice invertido apresentado no Capítulo 8 que problemas podem causar os sintomas e sinais percebidos. Você terá em mãos uma lista de hipóteses. Em seguida, consulte os problemas referenciados no catálogo de problemas. Um deles pode estar ocorrendo em sua rede. Ao consultar os problemas você pode optar por tentar confirmá-los (Seção **TESTES CONFIRMATÓRIOS**) ou por buscar novas informações (Seção **SINAIS**).

Quando quiser recuperar uma determinada informação de gerência e não souber como fazê-lo, um dos procedimentos pode ajudar. Os procedimentos apresentados no Capítulo 9, em especial, são bastante genéricos: informam como conectar um analisador de protocolos à rede e como obter uma interface de linha de comando em um equipamento de interconexão.

O catálogo de problemas (Parte II) pode também ser lido seqüencialmente. À medida que procedimentos forem referenciados você pode escolher consultá-los. Após a leitura, você terá aumentado sua bagagem de experiências e conhecimentos. Será como se você já tivesse vivido cada problema apresentado. É uma boa forma de adquirir experiência sem sofrimento.

Para entender bem cada problema do catálogo é preciso ter conhecimentos básicos sobre o assunto abordado. Cada problema referenciará um apêndice que deverá ser lido caso o leitor não conheça o assunto. Se você não sabe para que serve e como funciona o protocolo de árvore de cobertura, por exemplo, você terá dificuldades em entender problemas relacionados a este protocolo.

SOBRE REFERÊNCIAS ON-LINE

Em alguns capítulos você encontrará referências que podem ser acessadas através da Internet. Nós garantimos que todas estas referências estão funcionando (link correto) em novembro de 2002. No entanto, mudanças em sites são bastante comuns atualmente, sendo possível que, mais tarde, infelizmente alguns dos links referenciados no livro estejam quebrados. Se isto ocorrer um dia a dica é: ir na página principal do site em questão e pesquisar pelo título da referência ou ir direto no link para publicações, recursos ou biblioteca digital e procurar pelo que você deseja.

LEGENDA

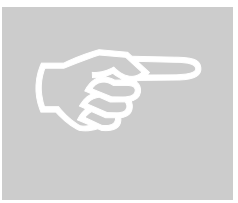
Durante a leitura deste livro você encontrará alguns estilos diferentes de fontes e ícones ilustrativos. Na Tabela 1-1 apresentamos uma legenda com o significado de alguns destes estilos.

Estilo	Significado
	Ícone usado para enfatizar uma boa prática de gerência, em geral, de configuração.
	Ícone usado para chamar a sua atenção para certos aspectos.
	Ícone que indica início de um exemplo que servirá para esclarecer melhor o entendimento de algo.
`comando`	Estilo para apresentação de comandos.
comando iterativo	Estilo usado para diferenciar respostas de comandos e comandos quando se tratam de comandos iterativos.
Destaque	Estilo usado para destacar palavras ou frases chave de um parágrafo. É usado para destacar sintomas e sinais de um problema.
Sinal diferencial	Estilo usado para indicar um sinal diferencial, cuja existência confirma um determinado problema.
$TTL	Estilo usado para representar algo que deve estar escrito em um arquivo.
/etc/resolv.conf	Estilo que representa nomes de arquivos.
Menu	Estilo que indica itens de interfaces amigáveis como as do Windows: menu, botões, etc.
equações	Estilo para apresentação de equações.
ifInErrors	Estilo para representar nomes de variáveis de MIBs (*Management Information Base*).

Tabela 1-1: Legenda de estilos encontrados no livro.

SUMÁRIO

Parte I
Introdução

Capítulo

1

1. RESUMO

Este capítulo está dividido em três grandes seções: introdução à gerência de redes, organização típica de uma equipe de gerência e analogia entre Gerência de Redes e a Medicina.

Na primeira seção oferecemos uma breve introdução à gerência de redes. Para manter o bom funcionamento de uma rede de computadores é necessário o auxílio de instrumentação adequada: uma ou mais estações de gerência que mostrem o mapa da rede e estatísticas como taxa de erros, de colisões, estado operacional de equipamentos e interfaces, dentre outras; analisadores de protocolos e outras ferramentas de gerência como `ping`, `traceroute` e `netstat`. É preciso também saber utilizar estas ferramentas e saber interpretar os dados de gerência obtidos com elas. Para muitas informações de gerência estabelecemos limiares que, quando ultrapassados, indicam problemas e podem gerar alarmes.

Na segunda seção mostramos a organização típica de um time de gerência. O *help desk* é responsável por ouvir reclamações de usuários sobre recursos de tecnologia da informação, consertar problemas, repassando para outros técnicos aqueles que não pode solucionar. A equipe de suporte técnico é a responsável final pela manutenção e configuração da rede. O operador da rede é responsável por receber os alarmes gerados pela estação de gerência. Existe ainda o gerente da equipe, que dirige e monitora o desempenho dos membros da equipe. Esta divisão não é obrigatória. É possível que uma ou duas pessoas apenas formem a equipe e acumulem para si todos os papéis apresentados.

Finalmente, a analogia entre a Gerência de Redes e a Medicina é apresentada na terceira seção deste capítulo. Um gerente de redes pode ser considerado o médico da rede, capaz de tratar as possíveis doenças (problemas apresentados pela rede) que possam surgir.

1 Introdução à Gerência de Redes

Nas próximas seções deste capítulo uma introdução básica à Gerência de Redes de Computadores, a organização típica da equipe de gerência em uma empresa e uma analogia entre a Medicina e a Gerência de Redes que nos acompanhará durante todo o livro.

1.1 Introdução à Gerência de Redes de Computadores

O objetivo da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede [STALLINGS].

A arquitetura geral dos sistemas de gerência de redes apresenta quatro componentes básicos: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência. A seguir falaremos um pouco sobre cada um deles:

- os elementos gerenciados possuem um *software* especial chamado agente. Este *software* permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência;

- em um sistema de gerência de redes deve haver pelo menos uma estação de gerência. Em sistemas de gerência distribuídos existem duas ou mais estações de gerência. Em sistemas centralizados – mais comuns – existe apenas uma. Chamamos de gerente o *software* da estação de gerência que conversa diretamente com os agentes nos elementos gerenciados, seja com o objetivo de monitorá-los, seja com o objetivo de controlá-los. A estação de gerência oferece uma interface através da qual usuários autorizados podem gerenciar a rede;

- para que a troca de informações entre gerente e agentes seja possível é necessário que eles falem o mesmo idioma. O idioma que eles falam é um protocolo de gerência. Este protocolo permite operações de monitoramento (leitura) e controle (escrita);

- gerentes e agentes podem trocar informações, mas não qualquer tipo de informação. As informações de gerência definem os dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerente e agente conversam.

Na Figura 1-1 vemos roteadores, comutadores[2], repetidores, impressoras, servidores e estações clientes. Todos estes equipamentos podem ter agentes instalados (idealmente terão). A estação de gerência deve obter informações de gerência destes agentes usando o protocolo SNMP.

---

[2] Consideramos que comutadores são equipamentos que realizam todas as tarefas realizadas por pontes e apresentam ainda algumas funcionalidades adicionais como, por exemplo definição de VLANs (Virtual LANs). Não utilizaremos em nenhum momento a palavra ponte quando nos referirmos a equipamentos de interconexão que operam na camada de enlace. Exceto quando estivermos tratando de funcionalidades não suportadas pelas pontes, o que for dito para comutadores é válido também para pontes.

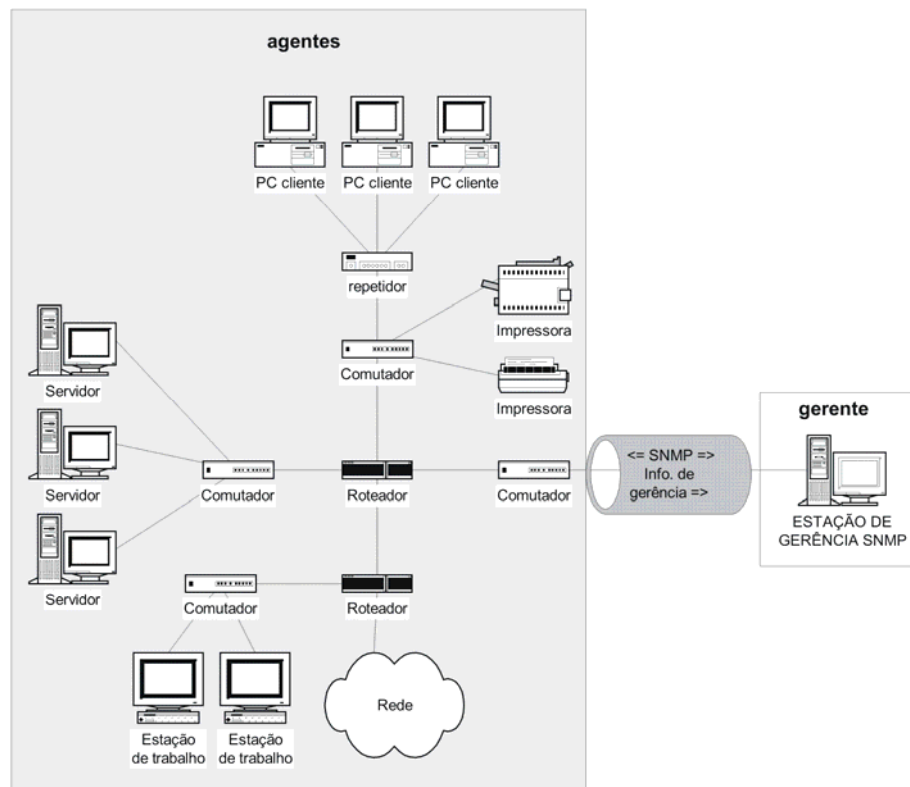



Figura 1-1: Elementos de uma arquitetura geral de solução de gerência.

A padronização de solução de gerência mais usada no mundo chama-se *Internet-Standard Network Management Framework*. Ela solução é mais conhecida como gerência SNMP. SNMP – *Simple Network Management Protocol* – é o protocolo de gerência deste padrão. Este padrão descreve não apenas o protocolo de gerência, mas também um conjunto de regras que são usadas para definir as informações de gerência e um conjunto inicial de informações de gerência que já podem ser utilizadas [ROSE].

Através da estação de gerência podemos obter informações tais como: taxa de erros, estado operacional de enlaces e equipamentos, utilização de enlace, dentre outras. Tão importante quanto obter estas informações é saber interpretá-las. Por exemplo, em um determinado momento, a estação de gerência informa que a taxa de erros de um certo enlace é 1%. Esta é uma taxa de erros aceitável?

Para muitas informações de gerência estabelecemos valores limites. Se o valor da informação obtida for maior que o limite estabelecido inferimos que algo anormal está ocorrendo na rede. Chamamos estes limites de limiares (*thresholds*). Assim, quando dizemos que limiares foram excedidos, estamos querendo dizer que obtivemos valores de informações de gerência que não estão dentro da faixa de normalidade e, portanto, são indicativos de problemas. Limiares excedidos e outros eventos podem gerar alarmes na estação de gerência. Quando a estação de gerência percebe que uma interface parou de operar, por exemplo, um alarme pode ser gerado.

Além do sistema de gerência de redes, outras ferramentas nos auxiliam a gerenciar uma rede. Dentre elas encontram-se analisadores de protocolos e

outras ferramentas mais simples como os comandos `ping`, `traceroute` e `netstat`, disponíveis sob vários sistemas operacionais.

Com os analisadores de protocolos podemos ver quais dados estão trafegando na rede. Eles nos permitem tirar um raio-X da rede, sendo, portanto, ferramentas importantes de gerência. Certas tarefas da gerência só podem ser realizadas com o auxílio de um analisador de protocolos.

Em todo o livro e, em especial, nos procedimentos (ver Seção 2.3) estaremos falando de estações de gerência SNMP, informações de gerência, limiares, analisadores de protocolos e outras ferramentas de gerência.

Nesta seção apresentamos uma brevíssima introdução à gerência de redes. Tentamos expor aqui apenas algumas definições que precisam ser entendidas antes que você continue a leitura deste livro. Se você sentir a necessidade de saber mais sobre a teoria de gerência veja algumas referências recomendadas na Seção **REFERÊNCIAS** no final deste capítulo. Leia mais sobre SNMP no apêndice 3. No apêndice 2 encontra-se uma breve introdução (e motivação para o uso) sobre ferramentas de gerência.

1.2 O papel do gerente de redes

Um dos objetivos da gerência de redes é prevenir e solucionar problemas na rede. Geralmente esta tarefa é realizada por uma equipe. Não existe uma regra rígida sobre os profissionais que fazem parte desta equipe. Cada organização tem autonomia para criar seu próprio time de gerência de redes de acordo com suas conveniências. Porém, é comum que nesta equipe existam profissionais que executem quatro tarefas distintas: o pessoal do *help desk*, o operador da rede, a equipe de suporte técnico e o gerente da equipe de gerência. Nesta seção iremos estudar as responsabilidades de cada um destes profissionais.

Quando os usuários enfrentam problemas relacionados à tecnologia de informação (os computadores nas suas mesas, aplicações, serviços, problemas na rede, etc.), eles pedem auxílio ao *help desk*. Em algumas organizações o *help desk* é composto por apenas uma pessoa, que atende chamadas telefônicas de usuários e tem certo grau de conhecimento para lidar com alguns problemas que forem reportados. Em organizações maiores, o *help desk* é composto por um grupo de pessoas um pouco mais especializadas, auxiliadas por aplicações que ajudam a gerenciar os problemas reportados (incluir novo problema, ver estado de problemas, criticalidade, etc.). Além disso, esta equipe pode ser auxiliada por outras ferramentas que ofereçam informações que possam ajudar a localizar e/ou solucionar problemas. Por exemplo, ferramentas que apresentam o estado operacional das interfaces e equipamentos da rede. Geralmente, esta equipe é capaz de solucionar os problemas mais simples e os erros cometidos pelos próprios usuários. Quando o *help-desk* existe, os usuários nunca (ou muito raramente) têm contato com a equipe de suporte técnico ou com o operador da rede, apenas com o *help-desk*.

Quando um usuário reporta um problema, o *help desk* solicita ao usuário algumas informações (mais detalhes serão apresentados na Seção 3.2), como por

exemplo, desde quando o problema está sendo observado e em que momentos do dia. Quando o *help desk* não é capaz de solucionar o problema em curto espaço de tempo, todas as informações coletadas são repassadas imediatamente a uma outra equipe: o pessoal do suporte técnico.

A equipe de suporte técnico é quem põe a mão na massa para solucionar os problemas mais abrangentes que surgirem ou que possam surgir e que não foram solucionados pela equipe de *help desk* ou pelo operador do sistema. É esta a equipe responsável pela configuração, operação e manutenção dos equipamentos da rede. Este é, portanto, o time que precisa possuir o maior nível de conhecimento técnico. Foi pensando mais especificamente neste pessoal que escrevemos este livro.

O operador do sistema é o profissional encarregado de acompanhar os alarmes gerados pela estação de gerência. Quando, por exemplo, um equipamento passa para o estado não operacional, o operador da rede perceberá um alarme na estação de gerência. Alarmes podem ser informados de diversas formas: mudança de cores no mapa da rede (o vermelho em geral indica problema), por *e-mail*, celular, etc. Quando o operador percebe que um problema está ocorrendo ou pode ocorrer, ele tenta resolver o problema ou o encaminha à equipe de suporte técnico.

O gerente da equipe de gerência de rede não é, necessariamente, um técnico em redes. O gerente tem um certo conhecimento em redes, mas não no nível do suporte técnico. Dentre as atividades deste gerente encontram-se: avaliar o desempenho da sua equipe de suporte, solicitar compra de equipamentos, aplicações ou outros recursos necessários, providenciar treinamento adequado para a equipe, reescalonar a solução de problemas para outros membros da equipe quando a solução demora, etc. Para avaliar o desempenho da equipe de gerência, o gerente pode se valer de certas métricas tais como: o tempo médio entre falhas e o tempo médio para correção de falhas na rede, percentual de problemas resolvidos em menos de 1 hora, entre outros.

É importante ressaltarmos novamente que esta divisão da equipe de gerência[3] de redes é comum, mas não obrigatória. Podem existir organizações pequenas onde o mesmo profissional acumula todas as tarefas descritas. É possível também que o próprio suporte técnico realize as tarefas do operador da rede. Em organizações maiores o suporte técnico pode ser dividido em primeiro e segundo níveis. Enfim, o importante é que você saiba que, na realidade, o profissional que chamamos neste livro de gerente de redes pode assumir vários papéis distintos em momentos distintos, mas geralmente, estaremos falando com a equipe de suporte técnico.

A Figura 1-2 ilustra os papéis mais comuns dos componentes da equipe de gerência de redes.

---

[3] Na realidade, o *help desk* não faz parte apenas da equipe da gerência da rede. Os usuários ligam para o *help desk* quando enfrentam problemas relacionados à tecnologia de informação, o que inclui problemas com a rede.

Em muitas organizações, além da equipe de gerência de redes existe a equipe de gerência de aplicações. Muitas vezes, a equipe de gerência de aplicações culpa a rede pelo mau desempenho de suas aplicações (e vice versa!). É, portanto, salutar que a equipe de rede colete informações da rede que possam ser apresentadas à equipe de gerência de aplicações quando necessário, para provar (ou não) que tudo está bem com a infra-estrutura de rede. Utilização de enlaces e taxa de erros são dados sempre interessantes.

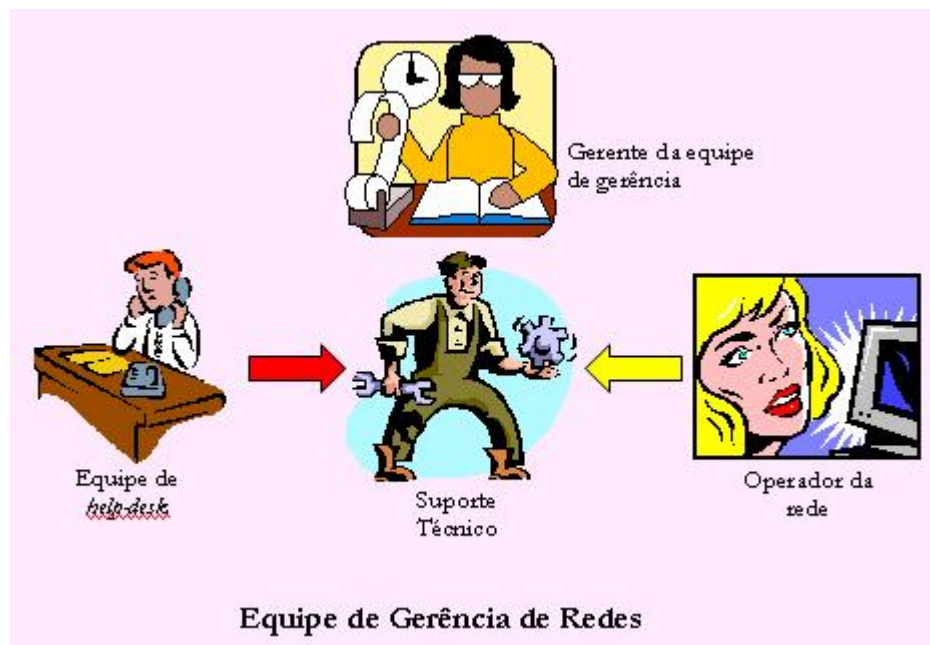



Figura 1-2: Uma equipe de gerência de redes de computadores.

1.3 Você: o médico da rede

Você já se deu conta de que você é um médico? Não é bem aquele médico que consultamos quando estamos doentes. Na realidade, você é um médico diferente. O seu paciente é a rede que você gerencia.

No dicionário, a primeira definição da Medicina é: "Arte e ciência de prevenir e curar as doenças". Qual seria a arte e ciência responsáveis por prevenir e solucionar os problemas da rede? Não seria a Gerência de Redes? Vamos adequar esta definição de Medicina e criar uma definição para a gerência de redes: "Arte e ciência de prevenir e solucionar os problemas da rede". A diferença entre um médico e uma pessoa responsável pela gerência de uma rede é que o paciente do médico é um ser humano, enquanto o paciente do gerente de redes é a rede. Felizmente, nossa realidade não é tão árdua quanto a dos médicos reais: não existem problemas sem solução. Ela pode ser cara, ser complexa, mas sempre existe.

Percebendo esta semelhança com a Medicina, podemos escrever os problemas de redes – que apresentaremos na Parte II do livro – baseados nesta analogia, apresentada na Tabela 1-1.

Medicina	**Gerência de Redes**
Muitas doenças podem ser prevenidas, outras não. Por exemplo, a AIDS é uma doença que pode ser prevenida, já a leucemia não.	Um problema de rede é para nós, gerentes, o que uma doença é para um médico. Alguns podem ser prevenidos quando utilizamos boas práticas de projeto e configuração e manutenção de redes, outros não. Um problema de rede é algo que deve ser consertado diretamente. Um roteador com configuração errada, por exemplo. Rede lenta e falta de conectividade não são problemas, elas não são consertadas diretamente. Elas são manifestações da rede devido a um problema. Ao se consertar o problema, estas manifestações devem cessar.
Quando estamos doentes vamos ao médico. A primeira pergunta que ele nos faz é: o que você está sentindo? Em geral, respondemos esta pergunta descrevendo o que o médico chama de sintomas. No dicionário, a palavra sintoma tem o seguinte significado quando empregada à Medicina: "*Qualquer fenômeno de caráter subjetivo provocado no organismo por uma doença, e que, descritos pelo paciente, auxiliam, em grau maior ou menor, a estabelecer um diagnóstico*".	Para nós um sintoma tem o mesmo significado, mas, como a rede não fala, os usuários é que os descreverão. Quando a rede está com problemas o pessoal do *help-desk*[4] receberá bastantes ligações. São os usuários reclamando que a rede está lenta, que não conseguem enviar *e-mails* ou que a rede não está funcionando. No contexto da gerência, sintomas são as conseqüências de um problema para os usuários. Rede lenta e falta de conectividade são exemplos de sintomas de problemas.
Após conversar com o paciente e descobrir o que ele está sentindo, o médico realiza alguns exames e observações em busca de sinais. Quem nunca foi para um otorrinolaringologista[5]? Com instrumentação adequada ele vai realizar certos exames (o exame da garganta é certamente o pior deles). Com estes exames o médico obtém mais informações, que irão lhe auxiliar a chegar ao diagnóstico correto. Estes exames só podem ser realizados pelo	Em uma rede não é diferente. Os usuários – assim como os pacientes – podem observar certos sintomas. Mas só o time de gerência está instrumentado e capacitado para coletar e interpretar informações mais "íntimas" da rede: os sinais. Por exemplo, um usuário nunca ligaria dizendo que a rede está lenta porque a taxa de colisões no domínio de colisões do qual participa está muito elevada. Em primeiro lugar porque ele provavelmente não sabe o que são colisões. Em segundo, ele não sabe como calcular esta taxa e não tem instrumentos adequados para tal. Por fim, e não menos

[4] Ou outro profissional com o qual os usuários da rede entrem em contato para fazer reclamações.

[5] Médico que trata de doenças de ouvido, nariz e garganta.

médico, que tem instrumentação e/ou procedimentos adequados para coletar certas informações, e conhecimentos suficientes para interpretá-las.	importante, ele não sabe o limiar para a taxa de colisões. Quanto é muito? 25%? Ele não sabe. Os sinais de que um problema existe são os mais diversos: taxa de colisões elevada, tráfego de difusão em excesso, taxa de erros elevada, dentre outros. Um gerente só é capaz de obter informações de gerência com instrumentação adequada. Após obtê-las, o gerente precisa saber interpretá-las, isto é, precisa identificar quando estão com valores estranhos, tornando-se sinais.
Certas doenças apresentam sinais típicos, cuja existência confirmam o diagnóstico sem a necessidade de testes adicionais. Na Medicina, estes sinais são chamados patognomônicos.	Problemas de rede também podem apresentar sinais patognomônicos. Chamaremos estes sinais de sinais diferenciais. Quando o sinal diferencial é encontrado nenhum teste confirmatório é necessário. Já achamos o problema.
Para dar o diagnóstico diferencial quando os sintomas e sinais coletados, por si só, não confirmam uma determinada doença, o médico precisa realizar alguns testes para confirmar ou negar suas suspeitas. Por exemplo, após os exames, o médico está em dúvida entre dois diagnósticos. Então ele vai realizar outros testes ou exames que possam confirmar uma das hipóteses e negar as demais.	Muitos problemas de redes podem causar sinais e sintomas bastante semelhantes, sendo impossível distinguir, antes de uma análise mais detalhada, que problema está ocorrendo. Quando não formos capazes de identificar o problema com os sintomas e sinais reunidos, devemos realizar testes confirmatórios. Por exemplo, após analisar os sintomas/sinais, podemos ficar em dúvida entre um cabo danificado ou uma interface defeituosa. Então, precisamos testar cada uma destas suspeitas para, enfim, chegar ao diagnóstico.
Muitas vezes uma doença pode ser descoberta antes mesmo dos seus sintomas se manifestarem. Por exemplo, em um exame de rotina no ginecologista, uma mulher pode descobrir que está com câncer de ovário, apesar de nenhum sintoma ter se manifestado ainda.	É possível que um problema seja detectado na rede antes mesmo dos usuários o terem percebido. Este é o objetivo da gerência de redes pró-ativa. Numa rede bem administrada, problemas de rede devem ser de conhecimento da equipe de gerência *antes* que os usuários percebam problemas. (pelo menos quando o problema afetar mais do que uma simples estação de trabalho). Numa empresa onde os problemas são descobertos apenas com reclamação de usuários, a equipe de gerência não está fazendo um bom trabalho. A rede em si pode ser um paciente, se adequadamente instrumentada. Ela mesma "fala" que está doente.

Tabela 1-1: Analogia entre a Medicina e a Gerência de Redes.

1.4 Referências

1.4.1 Livros

[HARNEDY] Harnedy, S., Harnedy, S. J. Total SNMP: Exploring the Simple Network Management Protocol. Segunda Edição. Editora Prentice Hall, Agosto, 1997.

[MAURO & SCHMIDT] Mauro, Schmidt. Essential SNMP. O'Reilly and Associates, 2001.

[ROSE1] Rose, T. M. The Simple Book: An Introduction to Network Management. Segunda Edição. Editora Prentice Hall, Março, 1996.

[ROSE2] Rose, T.M., McCloghrie, K. How to Manage Your Network using SNMP: The Network Management Practicum. Editora Prentice Hall, Janeiro, 1995.

[STALLINGS] Stallings, W. SNMP, SNMPv2, SNMPv3 and RMON1 and 2. Terceira Edição. Editora Addison-Wesley, 1998.

2. RESUMO

No catálogo de problemas você encontrará informações sobre 37 problemas, classificados por camada OSI, que podem ocorrer em uma rede de computadores. Para cada um destes problemas apresentamos:

- uma descrição do problema;
- efeito negativo do problema observado pelos usuários da rede (sintomas);
- comportamentos ou características internas da rede que podem ser observadas pelo time de gerência com instrumentação adequada (sinais). Para cada sinal apresentado existe um procedimento que informa como obtê-lo;
- testes adicionais que podem confirmar o problema;
- sugestões de como solucionar o problema.

2 Introdução ao catálogo de problemas

Apesar do título, neste capítulo introduzimos não apenas o catálogo de problemas (Parte I), mas também os procedimentos (Parte II). Na primeira seção apresentamos um breve resumo da analogia entre a Medicina e a Gerência de Redes, para aqueles que não leram o Capítulo 2. Na seção seguinte apresentamos o que é o catálogo de problemas, como ele está organizado, por que ele está organizado assim e o que são os índices invertidos. Por fim, definimos os procedimentos e sua organização.

2.1 Analogia entre a Gerência de Redes e a Medicina

Na Tabela 2-1 apresentamos um pequeno resumo da analogia entre a Gerência de Redes e a Medicina. Para obter mais detalhes consulte a Seção 1.3.

Medicina	**Gerência de Rede**
Sintomas: o que um paciente sente quando está doente.	Sintomas: o que o usuário da rede sente quando um problema está ocorrendo.

Sinais: informações sobre o estado/comportamento do paciente obtidas pelo médico através de exames e/ou observações.	Sinais: informações sobre o estado/comportamento da rede obtidas pelo gerente da rede com o auxílio de instrumentação adequada.
Sinais patognomônicos: sinais cuja existência já confirmam a existência de uma certa doença.	Sinais diferenciais: sinais cuja existência confirmam um certo problema.
Testes confirmatórios: testes que o médico precisa realizar para chegar ao diagnóstico diferencial quando estiver suspeitando de várias doenças.	Testes confirmatórios: testes que o gerente de redes precisa realizar para confirmar ou negar um ou mais problemas.

Tabela 2-1: Resumo da analogia entre a Medicina e a Gerência de Redes.

2.2 O catálogo de problemas

O catálogo de problemas é uma coletânea de 37[6] problemas que podem ocorrer em uma rede. Como a metodologia de detecção de problemas que seguimos (ver Capítulo 3) sugere que as hipóteses sejam testadas por camadas – da camada física em direção à camada de aplicação – os problemas foram agrupados no catálogo por camada OSI.

Um problema é algo que se deve consertar diretamente, como um cabo com conector frouxo ou uma configuração errada de um roteador. Rede lenta, por exemplo, não é um problema, pois não se conserta a lentidão da rede diretamente. Rede lenta é, sim, um sintoma de um problema. Ao consertar o problema, os sintomas não mais devem ser percebidos.

No catálogo de problemas desta edição encontramos os problemas apresentados na Tabela 2-2.

Levando em consideração a analogia com a Medicina e a metodologia para detecção, diagnóstico e resolução de problemas (que será apresentada no capítulo a seguir), um problema tem 5 elementos essenciais:

1. Descrição

    Na descrição de um problema serão apresentadas as circunstâncias em que o problema surge. Algumas vezes poderão também ser apresentadas causas mais comuns e subconjuntos mais específicos deste problema. Se fosse uma doença, a descrição (resumida) de resfriado seria: processo inflamatório causado por vírus ou por vírus associados a outros microrganismos ou, ainda, de natureza alérgica. A descrição é importante para que você entenda o problema. Ao ler a descrição você já começará a ter uma boa idéia do reflexo do problema na rede, pois você o terá entendido.

[6] Pretendemos aumentar o número de problemas incluídos no catálogo a cada nova edição do livro.

Camada Física	▪ **Cabo rompido ou danificado;** ▪ **Conector defeituoso ou mal instalado;** ▪ **Descasamento de modo e/ou velocidade de operação;** ▪ **Equipamento de interconexão defeituoso;** ▪ **Placa de rede ou porta de equipamento de** interconexão defeituosas; ▪ **Interferência no cabo;** ▪ **Saturação de banda em segmentos Ethernet compartilhados;** ▪ **Tipo errado de cabo;** ▪ **Violação de regras de cabeamento** Ethernet;
Camada de Enlace	▪ **Interface desabilitada;** ▪ **Problema com árvore de cobertura;** ▪ **Saturação de recursos devido a excesso de quadros** de difusão; ▪ **Tempo de envelhecimento de tabelas de endereços inadequado;** ▪ **Validade da cache ARP inadequada;**
Camada de Rede	▪ **Tabela de rotas de hospedeiros incorretas;** ▪ **Endereço IP de hospedeiro** incorreto; ▪ **Hospedeiro com máscara de rede incorreta;** ▪ **Cliente DNS mal configurado;** ▪ **Servidor DHCP mal configurado;** ▪ **Rotas estáticas mal configuradas;** ▪ **Equipamento inserido em VLAN incorreta;** ▪ **VLANs não estão configuradas;** ▪ **Comutadores não conseguem trocar informações sobre VLANs entre** si; ▪ **Ambiente RIP-1 com VLSM** e/ou redes não contíguas; ▪ **Diâmetro RIP** com mais de 15 roteadores; ▪ **Roteadores RIP-2 não enviam ou** recebem pacotes RIP-1; ▪ **Tráfego RIP saturando largura de banda** ▪ **Filtro IP não** permite a passagem de tráfego RIP (UDP 520);
Camada de Aplicação	▪ **O serviço de nomes não** está habilitado; ▪ **DNS: descasamento de registros A e PTR em** arquivos de zonas; ▪ **Inconsistência entre registros dos servidores DNS primário e** secundários; ▪ **O TTL default** de uma zona DNS não está configurado; ▪ **DNS: TTL e outros campos do registro SOA** com valores inadequados; ▪ **Falta "." após nomes totalmente qualificados em registros** DNS; ▪ **Filtro IP barrando** tráfego DNS; ▪ **Servidor de correio eletrônico com repasse totalmente aberto;**

	▪ **Servidor de correio eletrônico com repasse totalmente fechado**;

Tabela 2-2: Problemas organizados por camada OSI trazidos nesta edição.

2. Sintomas

Os sintomas de um problema informam o que os usuários da rede podem perceber como conseqüência da existência do problema. Em outras palavras, os sintomas descrevem o efeito negativo do problema para os usuários. Sintomas típicos de problemas em rede são: a rede está lenta, a rede não está funcionando, um determinado serviço está indisponível. Lembre-se que você também é usuário da rede e, como tal, pode perceber os sintomas.

3. Sinais

Os sinais são características mais internas da rede que têm seu estado normal alterado em conseqüência da existência do problema. Os sinais, geralmente, não são percebidos pelos usuários, pois eles só podem ser obtidos com o auxílio de instrumentação adequada, como estações de gerência, analisadores de protocolos ou outras ferramentas de gerência. São manifestações adicionais, além das manifestações externas que se apresentam aos usuários.

Cada sinal referencia um procedimento. Cada procedimento informa pelo menos uma maneira de obter o sinal em questão. Falaremos mais sobre os procedimentos na Seção 2.3.

Alguns sinais podem não ser percebidos na fase de busca das informações, apenas na fase de testes. É possível ainda que o problema seja confirmado sem que todos os sinais apresentados sejam vistos. O objetivo deste campo é descrever características internas da rede que podem ser observadas quando um determinado problema estiver ocorrendo. Alguns sinais são facilmente percebidos quando utilizamos uma boa estação de gerência: taxa de erros, estado operacional de enlaces e equipamentos, dentre outros. Outros sinais só podem ser detectados com o auxílio de um analisador de protocolos ou uma interface de linha de comando. Além disso, é possível que em uma situação específica, você encontre sinais que não listamos aqui para um determinado problema.

4. Testes confirmatórios

Os testes confirmatórios indicam os passos que devem ser seguidos para confirmar ou negar a existência do problema de rede que está sendo apresentado. Quando sinais diferenciais forem encontrados, não será necessária a realização de testes adicionais para confirmar o problema.

5. Sugestões de tratamento

Nas sugestões de tratamento iremos sugerir soluções eficientes para o problema sendo descrito. O problema que foi confirmado deve ser

solucionado o mais rapidamente possível. A solução deve ser também correta, não introduzindo outros problemas na rede.

Além disso, em alguns casos, daremos sugestões de como proceder para evitar que o problema ocorra. Neste caso, além do tratamento indicamos a prevenção.

2.2.1 Por que um catálogo de problemas?

Neste momento, você pode estar se perguntando: por que essa turma escreveu um catálogo de problemas e não de sintomas? Esta é uma boa questão, que merece uma explicação.

Nosso intuito inicial foi criar um catálogo de sintomas. Mas, nossos primeiros estudos mostraram – e você perceberá isso ao ler o catálogo – que um sintoma pode ser causado por diversos problemas diferentes. O sintoma rede lenta, por exemplo, pode ser causado por um grande número de problemas. Além disso, um mesmo problema pode causar ora um sintoma ora outro. Ao considerar um catálogo de sintomas teríamos muito a falar sobre cada sintoma. Alguns problemas teriam que ser referenciados em um determinado sintoma e repetidos em outros sintomas. Não achamos didático misturar vários problemas desta forma.

Organizar o catálogo por sinal também não se mostrou uma boa idéia. Muitos sinais também se repetem em vários problemas diferentes, levando à mesma situação de um catálogo escrito por sintomas. Além disso, um único sinal (exceto quando ele é diferencial) pode não dizer muito sobre o problema. Existem problemas distintos em que o mesmo sinal se repete, e a existência de outro sinal é um fator chave para a localização do problema.

Decidimos então organizar o catálogo por problema, mostrando, para cada um deles os possíveis sintomas e sinais. A finalidade de um gerente de redes diante de uma notificação de um problema é descobrir e solucionar o problema, não os sintomas e sinais. Estes devem ser conhecidos para que o problema seja localizado. Os sinais e sintomas são o meio, não o fim.

Concordamos, no entanto, que uma tabela indexada por grupos específicos de sintomas e sinais ajudaria bastante na hora de criar hipóteses. Portanto, criamos os *índices invertidos*, onde cada grupo específico de sintomas ou sintomas/sinais referencia um ou mais problemas. Falaremos mais sobre os índices invertidos na seção a seguir.

Uma outra razão que nos leva a organizar o catálogo por problema diz respeito ao desenvolvimento e melhoramento futuros do catálogo. Da forma como ele está organizado, novos problemas podem ser inseridos e melhorados facilmente, pois já sabemos onde encontrá-los. Se o catálogo fosse de sintomas, modificações e adições não seriam tão simples. Precisaríamos encontrar os locais correto para inserir cada novo problema, já que estariam todos juntos, sendo referenciados pelo mesmo sintoma.

2.2.2 Os índices invertidos

Os índices invertidos são tabelas que nos ajudam a descobrir que problemas podem ser causados por determinados grupos de sintomas e sinais. No Capítulo 8 (último capítulo da Parte II do livro), você encontrará dois índices invertidos: o índice invertido de sintomas e o índice invertido de sintomas e sinais.

Os índices invertidos são particularmente importantes quando a rede que você gerencia estiver com problema. De posse dos sintomas e sinais coletados sobre o problema, você pode recuperar, através dos índices invertidos, que problemas podem estar ocorrendo na rede. Isto ficará mais claro no capítulo seguinte, quando apresentamos como o catálogo, os índices e os procedimentos podem ser usados em conjunto com uma metodologia para detecção, diagnóstico e resolução de problemas de rede.

2.3 Os procedimentos

Na seção anterior, quando falávamos de sinais, dissemos que cada sinal referencia um procedimento e cada procedimento ensina pelo menos uma maneira de se obter o sinal em questão. Nesta seção explicaremos o que queremos dizer com isso.

Para nós um sinal é uma informação interna ou característica da rede, que deve ser obtida com o auxílio de instrumentação adequada. Um procedimento ensina como obter um sinal e interpretá-lo.

Eis alguns exemplos de sinais: taxa de erros elevada, taxa de colisões elevada, requisições ARP sem resposta e resolução de nomes externos não funciona. Sobre todos os sinais podemos perguntar: como posso obtê-lo? Outras perguntas que podem ser feitas são: quando considero que seu valor está anormal? O que este sinal significa? Qual seria o comportamento normal? Os procedimentos têm o objetivo de responder estas perguntas.

Cada procedimento, assim como cada problema do catálogo, será apresentado de uma forma padronizada. Em seções chamadas **DESCRIÇÃO E DICAS** descrevemos o que o sinal significa, e, quando cabível, que valores do sinal são considerados anormais ou como deveria ser o comportamento normal da rede ou serviço envolvido. Na realidade, quando chamamos a informação de gerência de sinal, significa que o seu valor ou comportamento já não é normal. Desta forma, seria mais correto reescrever a frase anterior da seguinte forma: em seções chamadas **DESCRIÇÃO E DICAS** descrevemos o que a informação de gerência significa, e que valores ou comportamentos são considerados anormais, transformando-a em um sinal de problema.

A forma como a informação de gerência é obtida é, na prática, dependente do tipo de instrumentação que devemos usar. Para cada sinal apresentado, existe uma instrumentação mais adequada. Tentamos, no entanto, apresentar várias formas de obter cada sinal, uma vez que muitas equipes podem não possuir toda a instrumentação. Cada leitor tenta obter o sinal com os instrumentos de que dispõe.

Em seções chamadas **USANDO UMA ESTAÇÃO DE GERÊNCIA SNMP** apontamos que variáveis de gerência SNMP devem ser monitoradas e como devem ser combinadas a fim de se obter a informação de gerência em questão.

Seções chamadas **USANDO UMA INTERFACE DE LINHA DE COMANDO** explicam como obter a informação de gerência com o auxílio de uma interface de linha de comando: a interface oferecida pelo *software* dos equipamentos de interconexão. Para mais informações sobre interface de linha de comando veja o procedimento apresentado na Seção 9.2.

Se for possível ou necessário obter a informação de gerência desejada através de um analisador de protocolos, o procedimento a ser seguido será explicado em seções intituladas **USANDO UM ANALISADOR DE PROTOCOLOS**.

Pode ser ainda possível obter a informação de gerência com o auxílio de outras ferramentas de gerência, geralmente programas de computador ou hardware especial. Neste caso, o título da seção muda dependendo da ferramenta a ser apresentada. Se as ferramentas a serem utilizadas forem, por exemplo, `ifconfig` e `netstat`, a seção será intitulada **USANDO IFCONFIG E NETSTAT**.

Alguns sinais podem ser obtidos através de vários tipos de instrumentação, outros não. Podemos obter a taxa de erros com o auxílio de uma estação de gerência, de uma interface de linha de comando, de um analisador de protocolos e de outras ferramentas de gerência, como `netstat`. Por outro lado, só podemos analisar o endereço origem de quadros de difusão com o auxílio de um analisador de protocolos. Por esta razão, alguns procedimentos apresentarão todas as seções mencionadas aqui e outros não.

Resumindo: no catálogo de problemas descrevemos que sinais são reflexos de cada problema de rede e nos procedimentos indicamos como obter as informações de gerência correspondentes a estes sinais e como interpretá-las.

Capítulo

3

3. RESUMO

Neste capítulo apresentamos uma metodologia geral de detecção, diagnóstico e resolução de problemas de rede. Segundo esta metodologia, quando um problema ocorrer na rede precisamos inicialmente buscar informações sobre o comportamento da rede – os sintomas e sinais. Os Procedimentos podem ajudar nesta etapa. Com base nas informações coletadas, começamos a desconfiar de certos problemas (desenvolver hipóteses com o auxílio dos Índices Invertidos). O terceiro passo é testar as hipóteses levantadas iniciando por aquelas que envolvam problemas da camada física. Neste ponto os Testes confirmatórios dos problemas levantados devem ser realizados. Uma vez confirmado um problema, devemos elaborar uma boa solução (veja Sugestões de tratamento do problema confirmado), implantá-la e testá-la. Por fim, é importante que documentemos os passos seguidos para a localização e resolução do problema.

3 Metodologia geral de detecção, diagnóstico e resolução de problemas

Infelizmente, mesmo o melhor sistema de gerência de redes não pode evitar todas as falhas. Quando somos notificados de que algo errado está ocorrendo na rede, precisamos, assim como o médico, dar o diagnóstico diferencial. Precisamos localizar e solucionar o problema o mais rapidamente possível. Mas, como o problema é detectado e localizado? Nesta seção apresentaremos uma metodologia geral de detecção e localização de problemas de rede. Ao mesmo tempo, damos dicas de como o catálogo de problemas, os índices invertidos e os procedimentos podem ser usados em conjunto com metodologia.

Além desta metodologia, é muito importante a existência de uma boa e atualizada documentação da rede e de uma equipe especializada, com conhecimentos avançados sobre redes de computadores, para lidar com os problemas inevitáveis. Leia mais sobre documentação de rede no apêndice 5.

Ao apresentar a metodologia consideraremos os três papéis de gerência mencionados na seção anterior. Mas, todos eles podem ser realizados pela mesma pessoa. Depende de como a equipe de gerência está organizada.

A metodologia que será apresentada nas próximas seções está ilustrada na Figura 3-1.

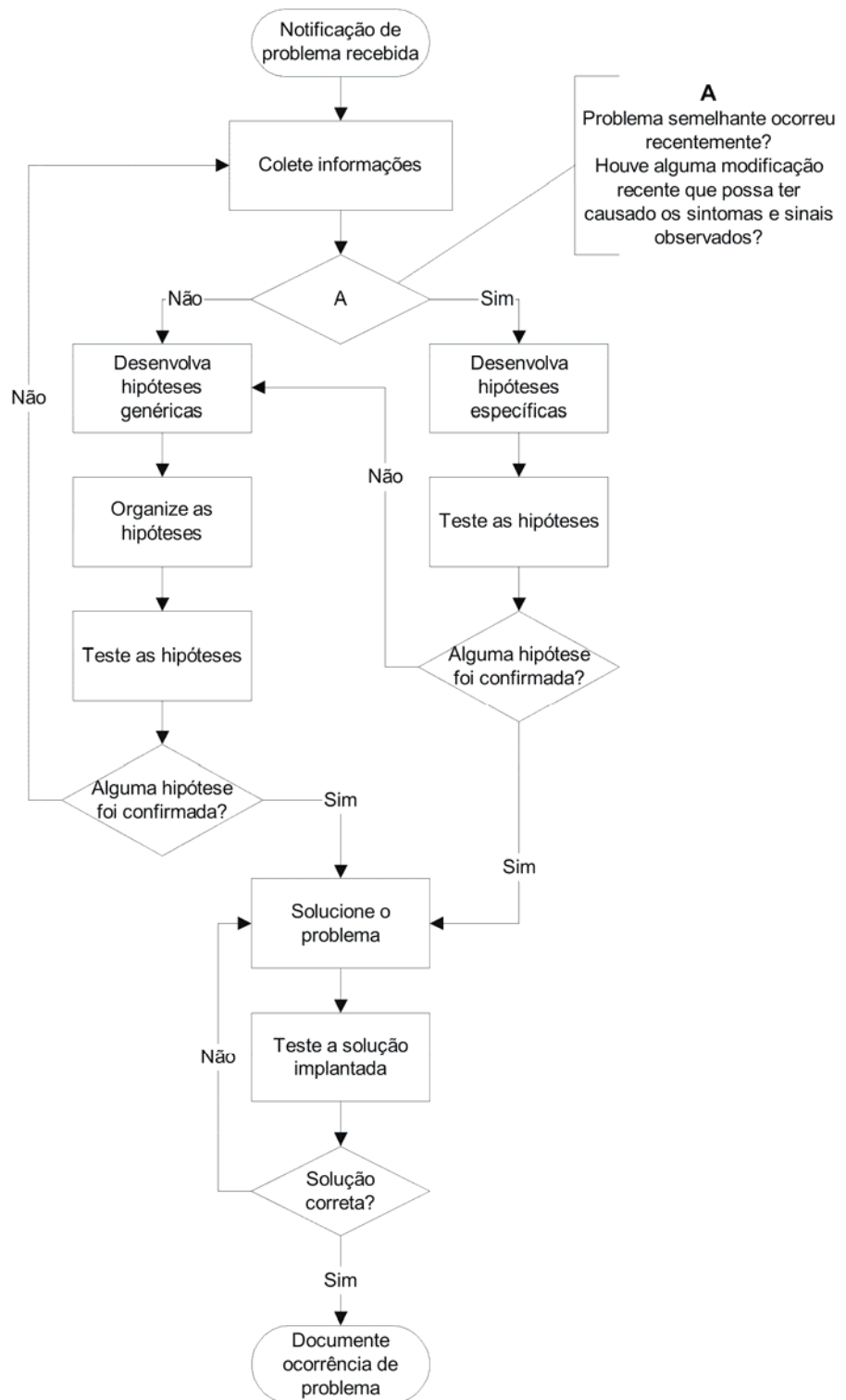



Figura 3-1: Fluxograma da Metodologia Geral de Localização e Resolução de Problemas de rede.

3.1 Detecção: a rede está apresentando comportamento estranho

Nesta etapa, a equipe de gerência é notificada de que algo estranho está ocorrendo na rede. A notificação pode ser feita de duas formas distintas:

os usuários ligam para o *help desk* e reportam sintomas de um problema;

o operador da rede percebe a existência de dispositivos ou interfaces não operacionais, limiares sendo excedidos ou padrões de tráfego estranhos. Estas situações podem gerar alarmes na estação de gerência. Quando o estado operacional de um equipamento crítico da rede muda para não operacional, o equipamento em questão pode mudar de cor no mapa da rede – ficar vermelho, por exemplo – ou um *e-mail* pode ser enviado ao operador do sistema.

Uma vez notificado sobre um problema, inicie imediatamente a fase de coleta de informações.

Não é interessante que problemas graves, que levem grande parte da rede a não funcionar, sejam descobertos através dos usuários. Uma das seguintes situações pode estar ocorrendo:

- não existe uma estação de gerência ou qualquer outra ferramenta de monitoração dos enlaces e equipamentos mais críticos da rede;
- existem ferramentas, mas muitos enlaces importantes não estão sendo monitorados, ou as ferramentas estão sendo utilizadas de forma errada;
- a ferramenta de gerência é maravilhosa, todos os enlaces e equipamentos críticos estão sendo monitorados, mas a equipe de gerência não analisa com bastante freqüência os dados apresentados por esta ferramenta.

Seja qual for a razão pela qual problemas graves estão sendo descobertos através de usuários, algo deve ser feito para reverter esta situação. O ideal é que somente problemas que envolvam um único usuário ou no máximo alguns usuários ligados a um mesmo repetidor/comutador sejam descobertos através deles.

3.2 Busque informações

Uma vez notificado sobre a existência de um problema, a primeira ação é buscar informações relevantes que possam ajudar a definir que problema está ocorrendo e onde ele está localizado.

Tente responder – seja com a ajuda dos usuários reclamantes, seja observando estatísticas e alarmes da estação de gerência – as seguintes questões:

Quem está sendo afetado pelo problema? Apenas um usuário? Todos os usuários? Alguns usuários que fazem parte de uma mesma sub-rede?

Quando o problema começou a ser percebido?

Desde então, o problema ocorre sempre, ou apenas em certos horários? Neste caso, em que horários?

O problema se manifesta sempre ou apenas quando alguma aplicação e/ou serviço específicos são usados? Neste caso, que aplicações e/ou serviços?

Alguma mensagem de erro está sendo gerada? Qual?

O problema é intermitente? Por exemplo, o usuário consegue enviar *e-mails* em certos momentos, mas em outros recebe mensagens de erro.

As informações obtidas sobre os problemas são passados para a equipe de suporte técnico através do *help desk*[7] ou através do operador da rede, quando estes não são capazes de resolver o problema em curto espaço de tempo.

Com base nestas informações, você pode iniciar a busca por outros sinais na estação de gerência ou usando outras ferramentas de gerência. É interessante que você obtenha o estado operacional dos equipamentos e interfaces envolvidas, taxa de erros e utilização de entrada e saída destas interfaces. Use a estação de gerência para obter o máximo de informações possível.

Se você não sabe como obter um sinal, procure ajuda nos **PROCEDIMENTOS**. Eles ensinam como obter – considerando vários tipos de instrumentação – e interpretar informações de gerência. Se você não possui uma estação de gerência monitorando os elementos críticos da rede e não tem ainda idéia de onde o problema possa estar ocorrendo, o procedimento apresentado na Seção 9.3 pode lhe ajudar.

Outras ferramentas de gerência úteis nesta fase são analisadores de protocolos, `ping` e `traceroute`. Em muitos casos, o problema pode envolver equipamentos ou serviços que não estão sendo monitorados pela estação de gerência. Outra possibilidade ocorre quando a quantidade de informação coletada não é suficiente para diagnosticar o problema. Além disso, no nível de gerência do qual estamos falando, não somos capazes de descobrir, através da estação de gerência, que um serviço está com problemas enquanto a infra-estrutura de rede sob a qual ele se apóia não está. Nestes casos, o auxílio de analisadores de protocolos e de outras ferramentas auxiliares é imprescindível.

Se o problema envolver um pequeno grupo de usuários, verifique a configuração de rede das máquinas de alguns deles. Elas podem revelar informações importantes.

As informações obtidas nesta etapa da metodologia nos deixam mais próximos do problema, levando-nos a focar a atenção onde o problema realmente está ocorrendo.

---

[7] Quando esta equipe existir e considerar que realmente existe um problema e não for capaz de solucioná-lo.

3.3 Recorrência de problema? Mudanças na rede?

Muitas perguntas já foram respondidas no passo anterior, mas deixamos duas, em especial, para ser respondidas nesta etapa:

- este problema ocorreu nos últimos 30 ou 60 dias?
    - se a resposta for "sim", grandes chances existem de o problema ter voltado a ocorrer;
- houve alguma modificação recentemente na rede que possa ter causado os sinais e sintomas verificados no passo anterior?
    - se a resposta for "sim", é muito provável que esta modificação tenha originado o problema reportado.

Respondendo positivamente a uma destas perguntas, vá direto ao ponto. Não perca tempo. Você muito provavelmente já localizou o problema, ou pelo menos já identificou que ele envolve um determinado serviço ou elemento da rede.

Suponha que você já descobriu que o problema envolve um certo serviço que foi instalado ontem. Você vai então criar uma lista de hipóteses, mas esta não levará em consideração hipóteses não relacionadas a este serviço. No fluxograma apresentado na Figura 3-1, dizemos que você deverá criar uma lista de hipóteses específicas.

Você já coletou informações sobre o problema, mas não criou uma lista genérica de hipóteses. Caso os testes que vêm a seguir não revelem que o problema era o imaginado, desenvolva hipóteses genéricas com base nos sintomas e sinais já reunidos.

Nesta etapa da metodologia, a documentação dos problemas já enfrentados poderá ser de grande auxílio (ver Seção 3.9).

3.4 Desenvolva hipóteses

Neste momento nós já temos informações suficientes sobre o problema para começar a desenvolver hipóteses. Até agora um problema foi apenas detectado, isto é, sabe-se de sua existência. Já temos também uma boa idéia de como a rede está reagindo ao problema (sintomas e sinais reunidos) e que partes da rede estão sendo afetadas. Com base em todas estas informações, podemos criar hipóteses sobre que problema pode estar ocorrendo. A pergunta básica a ser respondida neste momento é: que problemas podem causar os sintomas e sinais percebidos? A criação da lista de hipóteses é o primeiro passo para localizar especificamente o problema.

É importante ressaltar que, para conseguir criar a lista de hipóteses é necessário que tenhamos um bom conhecimento sobre como as redes e os serviços oferecidos por elas funcionam. É preciso saber como as coisas deveriam estar

funcionando se nenhum problema estivesse ocorrendo, comparar com o que está ocorrendo e perceber o que pode estar causando o comportamento atípico. Se você desconhece como o serviço DHCP funciona, não poderá jamais desvendar problemas que envolvam este serviço.

Além disso, precisamos também conhecer a rede que está sendo gerenciada. Onde estão os serviços, como deve ser o roteamento, como se dá a interconexão dos equipamentos e onde estão implantados *firewalls*, são exemplos de informações que devemos conhecer previamente.

Vamos voltar a nossa analogia com a Medicina. Para que um médico consiga, a partir de sintomas e sinais, suspeitar de certas doenças, ele precisa conhecer a anatomia e o funcionamento do corpo humano. Caso contrário, ele não conseguiria chegar ao diagnóstico diferencial.

Nesta etapa da metodologia os **ÍNDICES INVERTIDOS** podem auxiliar. Veja nos índices invertidos que problemas podem causar os sintomas e sinais observados. Desta forma, você obterá facilmente uma lista de hipóteses inicial.

Chegou o momento de exemplificarmos a metodologia sendo apresentada. Suponha que você tenha as seguintes informações:

- alguns usuários do Setor de Marketing ligaram para o *help desk* reclamando que a rede não está funcionando há 15 minutos. Nem *logon* na rede eles conseguem fazer;
    - estas foram as informações repassadas pela equipe de *help desk*;
- todos os equipamentos e interfaces monitorados pela estação de gerência estão operacionais e não apresentam limiares excedidos. Mas, existem repetidores que ligam máquinas clientes do Setor de Marketing à rede que não estão sendo monitorados;

Baseados nestas informações, consultamos o índice invertido de sintomas e sinais e desenvolvemos as seguintes hipóteses:

- cabo rompido ou danificado entre repetidores localizados no Setor de Marketing;
- conector defeituoso ou mal instalado entre repetidores localizados no Setor de Marketing;
- um ou mais repetidores defeituosos no Setor de Marketing;
- problema com o serviço DHCP do Setor de Marketing;
- problema com o serviço de nomes do Setor de Marketing;

Não se preocupe neste momento em identificar claramente o problema. O que você e sua equipe irão fazer nesta etapa é um *brain storm*. Irão levantar todas as possibilidades que vierem em mente. Se, no entanto, você estiver criando uma lista de hipóteses específicas, leve em consideração apenas o elemento da rede ou serviço que já estiver sob suspeita.

3.5 Organize a lista de hipóteses

Uma vez confeccionada a lista de hipóteses, classifique-as com base nas camadas do modelo de referência OSI. Reúna hipóteses relacionadas à camada física separadas das hipóteses relacionadas à camada de enlace e assim por diante. As hipóteses da camada física são as primeiras a serem testadas. Em seguida vêm as da camada de enlace e assim sucessivamente. Nos índices invertidos, os problemas já estão organizados por camada OSI.

Duas razões nos fazem iniciar os testes pela camada física: uma delas é que cita-se na literatura que 90% dos problemas de uma rede recaem em problemas de cabeamento [HAUGDAHL]; a segunda razão – não menos importante – é que se a camada física não está bem, as demais camadas também não estarão, pois dependem dela para seu bom funcionamento.

Retomando o exemplo citado na seção anterior, temos os seguintes grupos:

Camada física

- cabo rompido ou danificado entre repetidores localizados no Setor de Marketing;
- conector defeituoso ou mal instalado entre repetidores localizados no Setor de Marketing;
- um ou mais repetidores defeituosos no Setor de Marketing;

Camada de rede e aplicação

- servidor DHCP desativado[8];
- servidor DHCP com escopo incorreto;
- servidor de nomes desativado;

Gerentes mais experientes e que já conhecem profundamente a rede que gerenciam podem organizar esta lista de forma diferente, baseados na probabilidade de ocorrência de um problema. Com o tempo, acabamos definindo em nossa mente que problemas são mais prováveis de ocorrer na rede que estamos gerenciando e estes são os primeiros da lista. É claro que acidentes ocorrem, e quando erramos somos mesmo obrigados a organizar a lista por camadas e iniciar pela camada física. Se você criou uma lista de hipóteses específicas, você pode organizá-la segundo a probabilidade de ocorrência de cada problema.

Ao organizar esta lista, já devemos estar pensando em como os testes serão feitos. Muitas vezes, será necessário criar um plano de ação, para que não cometamos erros na próxima fase. Será necessário não apenas classificar os problemas por camada OSI, mas ordenar problemas de uma mesma camada. O que testar primeiro: o cabo de rede ou a placa de rede?

Com o tempo, você perceberá que fica mais fácil testar alguns problemas quando outros já tiverem sido testados. Por exemplo, alguns testes de

[8] Consideramos neste livro problemas com o serviço DHCP como sendo da camada de rede, pois este serviço está diretamente relacionado à configuração da camada de rede em hospedeiros.

diagnóstico da placa de rede envolvem testes de comunicação com o equipamento remoto. É, portanto, mais interessante que o cabo de rede ligado a esta placa seja testado antes da placa.

Problemas de uma mesma camada podem também ser organizados por probabilidade de ocorrência ou facilidade de teste. Cabe a você e a sua equipe decidir a ordem em que eles serão testados.

3.6 Teste as hipóteses levantadas

Na etapa anterior você organizou as hipóteses na ordem em que devem ser testadas. Nesta etapa você vai testar as hipóteses. Você vai simplesmente implementar o plano de ação de testes criado na fase anterior. Se as etapas anteriores tiverem sido bem realizadas, após esta fase você terá localizado claramente o problema.

Uma vez obtida a lista de hipóteses dos índices invertidos, consulte os problemas referenciados nela. Um por vez, iniciando pelos problemas da camada física (na ordem em que eles estão na lista). Para confirmar ou negar cada problema da lista basta seguir os **TESTES CONFIRMATÓRIOS** de cada problema. Nos testes confirmatórios, assim como nos procedimentos, tentamos apresentar testes alternativos, para quem não tem a ferramenta apropriada para confirmar o problema.

Caso nenhuma das hipóteses tenha sido confirmada, volte para o passo de busca de informações (Seção 3.2). Tente reunir mais informações sobre o problema e em seguida crie novas hipóteses, organize-as e teste-as. Faça isto até localizar claramente o problema.

Para não perder o controle do problema, realize um teste por vez. Muitos testes envolvem modificações, por exemplo, substituição de equipamentos ou cabos de rede. Se após a modificação os sintomas e sinais cessarem, o problema foi confirmado. Se você fizer duas modificações ao mesmo tempo e perceber que o problema foi resolvido, ficará sem saber qual era o problema, invalidando o seu teste. Portanto, nunca efetue mais de uma modificação por vez, o que implica também em nunca testar mais de uma hipótese por vez.

Voltemos ao exemplo já citado em seções anteriores. Suponha que você não tem um testador de cabos. Para descobrir o problema mais rápido você resolve trocar um repetidor suspeito e um cabo suspeito ao mesmo tempo. Após as trocas, os sintomas e sinais cessaram. Mas você ficará sem saber se o cabo estava com problema, ou o repetidor estava defeituoso.

Quanto mais bem equipado você estiver, mais rápidos e simples serão os testes. Por exemplo, testar problemas de cabeamento sem o auxílio de um bom testador de cabos pode ser uma tarefa bastante trabalhosa. É importante também que você tenha cabos de rede, placas de rede e equipamentos de interconexão sobressalentes que possam ser usados durante os testes e que possam substituir peças que estiverem com defeito.

Dica: se você desconfia de muitos problemas de camadas inferiores, um único teste pode negar todos eles, ou confirmar que um deles existe, infelizmente, sem revelar qual. Para realizar este teste use `ping`. Suponha que um usuário reclamou que não consegue usar determinada aplicação de rede. Se a máquina deste usuário estiver com as configurações de rede corretas, você pode enviar `ping` para o servidor (usando o endereço IP do servidor, não o nome). Se obtiver resposta deste servidor (nenhum quadro for perdido e o tempo de ida e volta for normal) terá descoberto que há conectividade física e lógica (até camada de rede) com o servidor. Ao descobrir isso, você não precisará mais perder tempo testando as hipóteses da camada física levantadas. Apenas se não obtiver resposta, ou se a resposta do `ping` indicar que houve perda de datagramas ou tempos de ida e volta absurdos, as hipóteses da camada física, de enlace e de rede precisarão ser testadas, pois você terá descoberto que o problema é realmente em camadas inferiores.

3.7 Solucione o problema

Neste momento, o problema já foi confirmado, e você deve solucioná-lo no menor prazo de tempo e da melhor forma possível. Olhe a Seção **SUGESTÕES DE TRATAMENTO** do problema que foi confirmado. Elas lhe darão dicas de como corrigir o problema da forma correta e, muitas vezes, como evitar que ele ocorra novamente.

Em algumas situações, a primeira solução (mais rápida) é paliativa. Pode ser uma solução temporária para que os usuários não fiquem mais tempo sem poder usar a rede. De qualquer modo, uma solução definitiva e correta deve ser elaborada.

Mais uma vez é como na Medicina: após dar o diagnóstico o médico irá tratar a enfermidade. Felizmente, na gerência de redes, todos os problemas têm solução. Elas podem ser caras, complexas ou demandar muito tempo para ser implantadas, mas sempre é possível solucionar um problema.

3.8 Teste a solução implantada

Não vá para casa satisfeito, certo de que resolveu o problema sem antes testar a solução implantada. Muitas vezes o cansaço nos leva a soluções aparentemente corretas, mas que não solucionam o problema, e, ao contrário, introduzem novos problemas.

Para testar sua solução use a rede, analise as estatísticas da estação de gerência. Se o problema foi descoberto através de reclamações dos usuários, use a rede a partir das máquinas destes usuários. Analise as estatísticas da estação de gerência, mesmo das redes onde nenhum problema foi reportado.

Fique ainda muito atento a toda a rede nos próximos 30 ou 40 minutos. Se a sua solução foi ineficaz, você perceberá neste intervalo de tempo. Se você descobrir que a solução não resolveu o problema, analise o que você fez e tente descobrir por que não deu certo. Você pode apenas ter esquecido de um detalhe bobo, ou

pode ainda ter que desfazer o que fez e elaborar uma nova solução. Neste caso, volte para o passo anterior (Seção 3.7).

Em casos mais raros (estes casos foram omitidos na Figura 3-1) é possível que você descubra que você solucionou um problema, mas ainda existe outro perturbando o bom funcionamento da rede. Neste caso, você pode decidir coletar mais informações, ou testar outras hipóteses que não foram testadas ainda, pois uma hipótese testada antes dela foi confirmada.

3.9 Documente suas atividades

Por fim, documente tudo. Documente as informações iniciais que obteve sobre o problema (o reflexo do problema na rede), as hipóteses levantadas, os testes e as soluções propostas. Se teve que voltar na metodologia em busca de novas informações para criar novas hipóteses, documente. Mesmo aquilo que não resolveu o problema deve ser documentado, pois ajudará outros (ou você próprio) a não repetir os mesmos erros. Essa documentação também pode lhe ajudar no futuro, caso o problema ocorra novamente.

Esta etapa não precisa ser feita, necessariamente, no fim. Geralmente, quando estamos tentando localizar um problema não queremos “perder tempo” com a documentação do mesmo. Então, esquecemos da documentação e pensamos apenas no problema que deve ser resolvido. Esta atitude pode dificultar a elaboração de uma boa documentação. Portanto, durante as fases anteriores, pelo menos anote – escreva frases curtas e objetivas – as ações realizadas. Assim você não esquecerá de informações importantes aqui.

Não temos a intenção de impor o uso desta metodologia. Ela não é baseada em estudos formais e não há provas matemáticas de que seja esta a melhor, se é que existe uma! Com a prática, você perceberá que esta metodologia é intuitiva. Você passará a utilizá-la naturalmente e não mais perceberá tão claramente a divisão entre cada uma de suas etapas. Elas se misturam e se complementam de forma natural.

3.10 Referências

Outras metodologias ou estratégias para detecção, localização e resolução de problemas podem ser encontradas em:

[3COM] Network Troubleshooting Overview.

http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c1ovrvw.htm

[GUIA-ETHERNET] Spurgeon, C. E. Ethernet – O Guia Definitivo. Tradução Daniel Vieira, Editora Campus, 2000.

Capítulo

4

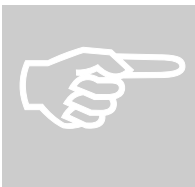
4 Problemas de nível físico

Neste capítulo encontram-se 9 problemas que podem ocorrer em uma rede relacionados à camada física: Cabo rompido ou danificado, Conector defeituoso ou mal instalado, Descasamento de modo e/ou velocidade de operação, Equipamento de interconexão defeituoso, Placa de rede ou porta de equipamento de interconexão defeituosas, Interferência no cabo, Saturação de banda em segmentos Ethernet compartilhados, Tipo errado de cabo, Violação de regras de cabeamento Ethernet.

4.1 Cabo rompido ou danificado

4.1.1 Descrição

A maioria dos enlaces de hospedeiros em redes locais (10Base-T e 100Base-TX, por exemplo) é formada por três componentes de *hardware*: uma placa de rede no cliente, uma porta em um equipamento de interconexão e um cabo conectando os dois primeiros componentes. Um cabo de rede, portanto, interliga dois ou mais componentes da rede. O rompimento de um cabo, conseqüentemente, impossibilita a comunicação entre os dispositivos da rede interligados por ele. Da mesma forma, cabos de redes danificados dificultam a comunicação entre os equipamentos unidos por ele.

Cabos de fibra ótica são os mais sensíveis. Quando flexionados além de um certo limite sofrem micro-fraturas, que não são visíveis externamente. As micro-fraturas causam uma maior perda de sinais no enlace. Curvas mais fechadas ou impactos muito fortes podem quebrar a fibra completamente. A tração ou torção excessivas da fibra durante a instalação também podem causar o seu rompimento.

Cuidado quando obras na rede hidráulica ou elétrica estiverem em execução. É mais freqüente que danos ou rompimentos em cabos ocorram quando trabalhos de deste tipo estão sendo realizados próximos aos cabos de fibra ótica aéreos ou terrestres. Por esta razão, quando estes trabalhos estiverem sendo realizados é recomendada uma atenção redobrada. Os técnicos da rede elétrica e hidráulica não conhecem a sensibilidade dos cabos óticos e por isso são, na maioria dos casos, responsáveis por causar fraturas e micro-fraturas nos cabos óticos.

Cabos de pares trançados também podem ter sua capacidade de transmissão prejudicada devido a torções, curvas muito acentuadas e nós apertados, pois estas formas de disposição do cabo alteram sua geometria. As alterações na

geometria do cabo podem causar prejuízos permanentes cuja gravidade depende da categoria do cabeamento utilizada.

Dispor cabos sobre objetos afiados, como por exemplo quinas de bastidores muito pontiagudas, é uma causa comum de curto circuito em cabos [LAN WIRING].

4.1.2 Sintomas

Cabos de fibra ótica quebrados completamente não permitem a passagem de sinais de uma extremidade a outra, inibindo o funcionamento da rede. Neste caso, os usuários reclamarão de falta de conectividade. Micro-fraturas tornam a rede lenta uma vez que causam uma grande quantidade de erros.

Pares trançados com geometria alterada podem causar falta de conectividade, conectividade intermitente ou ainda conexões lentas. Se o cabo danificado fizer parte do *backbone*, muitos usuários serão afetados.

Os usuários, em geral, reclamarão que a rede não funciona, ou alguns serviços não funcionam ou a que a rede ou alguns serviços estão muito lentos. Isto irá depender da localização do cabo com problema e do tipo de defeito no cabo.

4.1.3 Sinais

Procedimento
10.1

Um dos principais sintomas de cabeamento ruim é a taxa de erros elevada, principalmente erros de CRC. Desconfie de taxas de erros que não sejam muito próximas de zero. Em enlaces metálicos pode ser detectado no máximo 1 erro a cada 10^9 bits transmitidos e em enlaces óticos 1 erro a cada 10^{12} bits transmitidos.

4.1.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verificar LEDs;

TESTE 2

Testar o cabo sob suspeita com um testador de cabos;

Se não tiver um testador de cabos à disposição:

TESTE 3

- trocar o cabo por outro, ou

TESTE 4

- utilizar outra porta nos equipamentos de interconexão envolvidos.

Teste confirmatório 1

O primeiro teste é bastante simples: trata de verificar se os LEDs dos equipamentos de rede onde o cabo suspeito está conectado estão acesos. Praticamente todas as placas de rede mais novas e todas as portas dos equipamentos de interconexão possuem LEDs que acendem ao receber pulsos vindos do outro lado da conexão, seja para enlaces metálicos, seja para enlaces de fibra ótica.

Se os LEDs de ambos os lados da conexão acendem ao conectar o cabo e apagam ao desconectá-lo é pequena a probabilidade da existência de um cabo danificado ou rompido. Porém, conectores inadequadamente instalados, interferência eletromagnética e cabeamento inadequado podem fazer o cabo falhar e ainda assim os LEDs da conexão acenderem [STEINKE]. Se apenas o LED de um dos lados estiver aceso é quase certa a existência de problema no cabo. No entanto, a falha pode ser devido a danos no cabo, conectores mal instalados ou interferência no cabo.

Se um testador de cabos estiver disponível, o próximo teste pode confirmar ou negar a existência de problemas no cabo. E pode fazer ainda mais: pode indicar especificamente qual o defeito (se é problema no conector ou se é realmente um cabo rompido ou danificado).

Teste confirmatório 2

Teste o cabo (ou os cabos) sob suspeita com um testador de cabos.

Um TDR é um equipamento usado para caracterizar e localizar falhas em cabos metálicos (par trançado e coaxial, por exemplo). Um TDR realiza sua tarefa enviando pulsos ao longo do condutor e examinando os pulsos refletidos. A onda refletida revela situações indesejáveis, como curtos-circuitos, quebras e anomalias na transmissão devido a curvas, nós ou compressões excessivas [LAN WIRING]. Testadores de cabos TDR são, portanto, capazes de identificar e localizar problemas em cabos metálicos. Um testador de cabos é apresentado na Figura 4-1.

O OTDR é um equipamento que tem os mesmos objetivos do TDR, mas realiza testes em cabos óticos. Testadores de cabos OTDR são capazes de localizar exatamente o local da fratura em cabos de fibras óticas [LAN WIRING]. A Figura 4-2 apresenta um testador de cabo ótico.

Figura 4-1: DSP 4100 Digital CableAnalyzer da Fluke.

Figura 4-2: NetTekTM OTDR da Tektronix.

Se um testador de cabos não está disponível será ainda possível confirmar se existe ou não problemas com o cabo suspeito, mas não será possível determinar qual o problema. Para tal, os próximos testes podem ser úteis.

Teste confirmatório 3

Troque o cabo suspeito por outro confiável – um cabo de testes, por exemplo – para certificar-se de que os equipamentos envolvidos estão configurados corretamente e não apresentam defeitos físicos. Se com seta troca os sintomas e sinais descritos cessarem, a suspeita de problemas no cabo foi confirmada. Se após a troca os sintomas e sinais continuam sendo percebidos o problema existente na rede não está relacionado com o cabo de rede sob suspeita. Em outras palavras, você acabou de confirmar que não havia problemas com o cabo de rede[9].

Se não for factível trocar o cabo por outro (não há outro cabo para a substituição ou o cabo suspeito é subterrâneo e sobre ele existe uma avenida movimentada, por exemplo) você pode realizar o seguinte teste:

Teste confirmatório 4

Para realizar este teste você precisará de uma máquina de testes. Conecte a máquina de testes em uma das extremidades do cabo. Envie `ping` para o equipamento ligado à outra extremidade do cabo. Se este equipamento for um repetidor envie `ping` para um outro dispositivo ligado ao repetidor. Realize o mesmo teste conectando a máquina de testes no outro equipamento. Se o

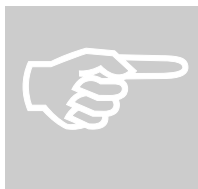
[9] É possível que a rede esteja apresentando dois problemas que causem os mesmos sintomas e sinais e que o cabo de rede substituído realmente estivesse com problemas. Mas a probabilidade disto ocorrer é bastante pequena.

resultado dos `pings` anunciar taxas de perda de pacotes maiores que zero em ambas as direções, o problema foi confirmado. Se em apenas uma direção o `ping` resultar em perda de dados, a suspeita recai sobre o equipamento ligado ao cabo (o que não é a máquina de testes).

Por exemplo: você suspeita de um cabo que liga dois comutadores entre si, comutador1 e comutador2. O cabo de rede utilizado para ligar estes equipamentos é cruzado – a porta de inversão está sendo utilizada. O teste é realizado em duas fases:

1. primeiro você desconecta o cabo suspeito de comutador1 e conecta na sua máquina de testes. A máquina de testes deve ser configurada com o endereço de rede e máscara de rede da rede onde ela vai ser conectada. Em comutador2 o cabo de rede suspeito está conectado em uma porta que participa da VLAN 1[10]. As máquinas desta VLAN são da rede 10.10.10.0/24. O endereço 10.10.10.13 não está sendo utilizado. Você configura a máquina de teste com este endereço e máscara 255.255.255.0. Enfim, envie `ping` para comutador2 (`# ping 10.10.10.2`) e analise o resultado;

2. na segunda fase, o cabo sob suspeita vai novamente ser conectado em comutador1. Você pode deixar a máquina de testes com a mesma configuração de rede. Desconecte comutador2 do cabo de rede suspeito, e em seu lugar conecte a máquina de testes. Envie `ping` para comutador1 (`# ping 10.10.10.1`) e analise o resultado.

Se houve perda de dados em ambas as fases do teste o problema foi confirmado. O cabo realmente está com problemas. Caso em apenas uma fase haja perda de dados, a suspeita passa para o equipamento conectado ao cabo. Se, por exemplo, apenas na primeira fase do exemplo apresentado houver perda de dados, comutador2 e a interface (de comutador2) à qual o cabo está conectado passam a ser suspeitos.

Algumas redes não utilizam um único tipo de cabeamento. Parte da rede possui cabeamento ótico e parte cabeamento metálico (par trançado, por exemplo). Neste caso conversores óticos podem ser utilizados. O conversor ótico simplesmente repete o sinal que chega de um enlace metálico em uma forma apropriada para transmissão em fibra ótica e vice-versa. O conversor ótico da Figura 4-3 foi projetado para conectar redes Ethernet 100Base-TX com Ethernet 100Base-FX.

[10] Configure a máquina de testes de forma que ela possa se comunicar na rede. Se VLANs por MAC estiverem definidas, o endereço MAC da placa de rede da máquina de teste deve ser cadastrado na VLAN adequada.

Figura 4-3: Fast Ethernet 100Base-TX/FX Converter da MFico.

Se o cabo suspeito na realidade é formado por mais de um tipo de cabo e um conversor entre eles (tal como um conversor ótico), é possível que o conversor esteja com defeito e que os cabos estejam intactos. O teste mais simples consiste em trocar o conversor por outro que esteja funcionando adequadamente (você provavelmente tem outros conversores de reserva ou para testes) e monitorar o enlace. Se os sintomas e sinais cessaram o problema no conversor foi confirmado.

4.1.5 Sugestões de tratamento

A solução para cabos metálicos é mesmo substituí-lo por outro devidamente instalado.

As fraturas em fibras óticas podem ser reparadas utilizando-se técnicas de *fiber splice*. [LAN WIRING]. Esta técnica consiste na junção, através de fusão ou utilizando um acoplador ótico, dos dois lados do cabo na quebra, sendo a fusão uma técnica que resulta em uma menor perda. Chame pessoas especializadas para realizar esta junção das fibras.

4.2 Conector defeituoso ou mal instalado

4.2.1 Descrição

No mundo das redes, um conector é a peça responsável pela ligação entre o cabo de rede e o equipamento de interconexão ou hospedeiro. É possível que conectores mal instalados ou defeituosos sejam a causa de problemas na rede que, em uma primeira análise, podem aparentar ser mais complexos.

Problemas em conectores RJ-45, utilizados em cabos de pares trançados, são mais comuns. As causas são diversas: a crimpagem pode ter sido mal feita, podem existir pares separados (*split pairs*), etc.

Em um cabo de pares trançados existem 4 pares de fios condutores. Os fios de cada par estão trançados entre si, como moléculas de DNA (forma helicoidal). Estas tranças são necessárias para reduzir a interferência elétrica entre os fios condutores. O fio 1 está trançado com o 2, o 3 com o 4 e assim sucessivamente.

Quando cabos de pares trançados são utilizados para comunicação Ethernet padrão (10Base-T e 100Base-TX), apenas os pinos 1, 2, 3 e 6 são utilizados[11]. Para evitar a interferência troca-se, em cada extremidade do cabo, a posição do fio 4 com o fio 6. Desta forma, todos os fios utilizados para transmissão e recepção de dados estarão trançados entre si, evitando interferências elétricas. Quando a troca entre os fios 4 e 6 não é realizada erros podem ser causados devido à interferência entre os fios condutores, causando o que se chama pares separados.

4.2.2 Sintomas

Os sintomas de conectores com problema podem ser diversos, depende do problema existente. O problema com conector pode causar mau contato com o equipamento ao qual o cabo está conectado, levando a conectividade intermitente. Em outras situações a conseqüência pode ser falta de conectividade ou rede lenta.

4.2.3 Sinais

Procedimento **10.1**

Conectores mal crimpados podem levar a um número elevado de erros, em especial erros de CRC [GUIA-ETHERNET, TIPS-ETHERNET] e de alinhamento. Deve-se sempre suspeitar de uma taxa de erros que não esteja muito próxima de zero.

Procedimento **10.2**

Taxa de colisões elevada. Uma taxa de colisões superior a 10% deve ser investigada. Conectores com problema também podem ser a causa de colisões excessivas[12] [TIPS-ETHERNET].

Procedimento **10.12**

Outras conseqüências de conectores mal instalados são *near-end crosstalk* (NEXT), que ocorre quando um sinal poderoso em um dos pares de fio é apanhado pelo par de fios adjacentes e atenuação do sinal [CABLETESTING-NEXT]. Uma boa ferramenta de certificação de cabeamento informa em que lado do cabo NEXT foi detectado. NEXT pode indicar também a existência de *split pairs* [HAUGDAHL].

4.2.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Use um testador de cabos para testar o cabo sob suspeita;

Se um bom testador não estiver disponível os seguintes testes podem ser realizados:

[11] Para 1000baseT (Gigabit Ethernet) são usados os 4 pares.

[12] Na tentativa de transmitir um quadro, após 16 colisões sucessivas a estação desiste da transmissão. Camadas superiores serão responsáveis pela solicitação da retransmissão do quadro.

TESTE 2

Verificar LEDs dos equipamentos conectados ao cabo com conector suspeito;

TESTE 3

Troque o cabo sob suspeita por outro que esteja funcionando apropriadamente;

TESTE 4

Use uma máquina de testes e a ferramenta `ping` para confirmar problemas no cabo;

TESTE 5

Realize uma inspeção visual no cabo de pares trançados;

Teste confirmatório 1

Use uma ferramenta de certificação de cabos para encontrar problemas no cabo. Bons testadores de cabos conseguem localizar exatamente onde está a falha. Se não for possível testar o cabo, oferecemos a seguir alguns outros testes que podem ser realizados para confirmar o problema.

Teste confirmatório 2

Tendo identificado o cabo com conector suspeito verifique se os LEDs dos equipamentos de rede onde o cabo está conectado estão acesos. Praticamente todas as placas de rede mais novas e todas as portas dos equipamentos de interconexão possuem LEDs que acendem ao receber pulsos vindos do outro lado da conexão, seja para enlaces de par trançado ou para enlaces de fibra ótica.

Em se tratando de cabos de pares trançados, ao verificar os LEDs chacoalhe o cabo próximo ao conector e verifique se a conectividade torna-se intermitente, isto é, se os LEDs ora acendem e ora apagam, dependendo da posição do cabo. Se você observar mau contato o problema com o conector está confirmado.

Se os LEDs de ambos os lados da conexão acendem ao plugar o cabo e apagam ao desconectá-lo é mais provável que o problema não seja no cabeamento, mas nos equipamentos envolvidos. Infelizmente, se isto ocorrer, não será possível confirmar o negar problemas nos conectores. É raro, mas conectores mal instalados, interferência eletromagnética e cabeamento inadequado podem fazer o cabo falhar e ainda assim os LEDs da conexão acenderem [STEINKE]. Se apenas o LED de um dos lados está aceso é quase certa a existência de problema no cabo. No entanto, a falha pode ser devido a conectores mal instalados, danos no cabo, interferência no cabo, etc.

Os mesmos testes confirmatórios 3 e/ou 4 do problema **CABO ROMPIDO OU DANIFICADO** podem ser realizados aqui. Eles irão ajudar a confirmar se o cabo sob suspeita está realmente com problema, mas não são suficientes para descobrir se o problema está relacionado aos conectores.

Teste 5

Em se tratando de cabos de pares trançados uma inspeção visual nos conectores pode ser feita facilmente. Assim, em alguns casos, mesmo que um testador de cabos não esteja disponível, é possível encontrar falhas em conectores.

A primeira dica é que apenas os 13mm finais de suas terminações podem ser destrançados. Quando mais que 13mm são destrançados, NEXT pode ser gerado.

A segunda dica é certificar-se de que os fios condutores estão todos em contato com os terminais metálicos do conector.

A terceira dica é desconectar e conectar o conector suspeito em uma porta de equipamento de rede e perceber se o conector é encaixado com dificuldade e ainda se ao conectá-lo ouve-se um pequeno estalo. Se o conector entrar na interface do equipamento com muita dificuldade, desconfie da crimpagem. Se você não ouve um estalo, também desconfie.

Busque também por pares separados. Eles geralmente são gerados quando as posições dos fios 4 e 6 não são trocadas entre si. Observe as cores das extremidades dos cabos. Se elas forem todas combinadas (fio branco/cor x sempre seguido pelo fio de cor x) é porque existem pares separados.

Sempre que suspeitar de conectores RJ-45 mal instalados analise os conectores em busca de possíveis falhas. Se encontrar alguma falha é muito provável que esta seja a fonte de seu problema.

Quanto maior o comprimento do cabo, a velocidade de operação e a sua utilização, piores os efeitos negativos causados por deslizes durante a instalação de conectores. Portanto, pode acontecer que um conector cujas falhas são vistas a olho nu funcione normalmente. É claro que ele não está de acordo com as especificações que devem ser seguidas por uma boa estrutura de cabeamento, mas muitos conectores, por exemplo com mais de 13 mm destrançados e desencapados, podem não causar mal algum. Por esta razão este não é um teste confirmatório. Estas são apenas algumas dicas que servem para aumentar ou diminuir as suspeitas com relação a um conector RJ-45.

4.2.5 Sugestões de tratamento

Instalar um novo conector, seguindo rigorosamente o padrão é a melhor solução para este problema. Se estiver usando conectores RJ-45, crimpá-lo novamente pode não solucionar o problema, pois é necessário a utilização de crimpadores especiais para a realização desta tarefa.

Se problemas com conectores costumam acontecer com freqüência é possível que o crimpador que você esta utilizando seja de má qualidade e a compra de um crimpador de melhor qualidade é então recomendada [LAN WIRING].

A Figura 4-4 mostra a seqüência de cores que deve ser seguida em cada uma das extremidades de um cabo (para cabos cruzados e cabos paralelos):

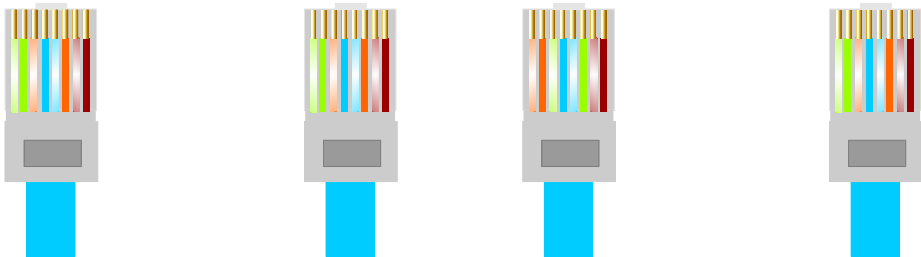



Figura 4-4: Terminação RJ-45 de ambas as extremidades para cabos cruzados e paralelos

Cabo paralelo		Cabo cruzado	
Pino RJ-45	Pino RJ-45	Pino RJ-45	Pino RJ-45
1 Tx +	1 Rx +	1 Rx +	3 Tx +
2 Tx –	2 Rx –	2 Rx –	6 Tx –
3 Rx +	3 Tx +	3 Tx +	1 Rx +
6 Rx –	6 Tx –	6 Tx –	2 Rx –

Figura 4-5: Terminação RJ-45 de ambas as extremidades para cabos cruzados e paralelos

Talvez você não esteja conseguindo visualizar as cores dos fios na figura acima. Afinal, ela está em preto e branco! ☺ Vamos dar uma colher de chá pra você. A seqüência de cores do cabo paralelo é:

- extremidade 1: branco_verde, verde, branco_laranja, azul, branco_azul, laranja, branco_marrom, marrom.
- extremidade 2: idêntica à extremidade 1.

Para o cabo cruzado a seqüência de cores é:

- extremidade 1: branco_verde, verde, branco_laranja, azul, branco_azul, laranja, branco_marrom, marrom.

- extremidade 2: branco_laranja, laranja, branco_verde, azul, branco_azul, verde, branco_marrom, marrom.

Existem outras padronizações que também são aceitas. Esta é a padronização EIA/TIA 568A que é indicada pelas normas de cabeamento estruturado e deve ser usada prefrencialmente.

4.3 Descasamento de modo e/ou velocidade de operação

4.3.1 Descrição

Leia mais sobre Ethernet no apêndice 1

O descasamento de modo de operação ocorre quando um lado de uma conexão Ethernet está configurado para trabalhar no modo *half duplex* e o outro em *full duplex*. Pode haver também descasamento de velocidade, quando um lado foi configurado para 100Mbps e o outro para 10Mbps. O modo e a velocidade de operação podem ser configurados manualmente pelo gerente da rede ou através da negociação automática.

A negociação automática é uma função opcional do padrão IEEE 803.2. Sua finalidade é permitir que dispositivos de rede diretamente conectados se comuniquem e negociem entre si a velocidade e o modo de operação, de forma que sua comunicação seja a mais eficiente possível. Existem padrões para detecção das velocidades 10 Mbps, 100 Mbps e 1000 Mbps e para os modos de operação *half* e *full duplex*.

O descasamento de velocidade ou modo de operação é mais comum quando um ou os dois lados estão configurados para a negociação automática, mas pode ocorrer também quando o administrador da rede modifica as configurações de um lado da conexão e esquece de corrigir o outro lado.

A idéia da negociação automática é muito boa, mas na prática ela não é perfeita. A negociação automática foi um dos últimos itens a ser adicionado no padrão, e antes dele ser aprovado, muitos fabricantes já haviam desenvolvido e implantado o seu próprio sistema de negociação automática. Além disso, não há padrão para a detecção automática quando a velocidade é 100 Mbps. O resultado deste desacordo é que uma interface pode detectar a velocidade e modo de operação do enlace de várias formas diferentes, e é freqüente que elas não sejam compatíveis entre si [KREIBICH]. Portanto, é comum que a detecção automática de velocidade ou modo de operação não funcione bem, principalmente entre equipamentos de fabricantes diferentes, sendo necessária a configuração manual.

Outra causa possível do descasamento é quando um lado está configurado para a negociação automática e o outro para operação *full duplex*, independente da velocidade. Neste caso, o lado que irá negociar encontrará a velocidade corretamente, mas será configurado para *half duplex* (que é o modo *default* quando a interface detecta que o outro lado não está configurado para a

negociação automática), gerando assim, descasamento de modo de operação [KEIBRICH].

4.3.2 Sintomas

Quando o problema é descasamento de velocidade o sintoma é falta de conectividade. Os usuários reclamarão que a rede ou parte dela não funciona ou que alguns serviços não estão disponíveis.

Quando o descasamento é do modo de operação existe conectividade, mas o desempenho da rede é prejudicado e a reclamação será de rede lenta. É possível que o problema de descasamento de modo de operação exista mas ninguém o perceba, principalmente se ocorre em enlaces com pequena utilização.

4.3.3 Sinais

Os tipos de erros irão variar dependendo do equipamento utilizado. Em geral, descasamento de modo de operação causa muitos tipos de erros em um enlace. Sinais indicativos de descasamento de modo de operação são:

Procedimento **10.1**

Número elevado de erros [KEIBRICH, BOURKE, TIPS-ETHERNET]. Os tipos de erros encontrados serão os mais diversos. Deve-se sempre suspeitar de uma taxa de erros que não esteja muitíssimo próxima de zero.

Procedimento **10.2**

Taxa de colisões superior a 10%. No lado da conexão que está operando em modo *full duplex* o protocolo CSMA/CD é desabilitado, pois neste modo de operação colisões nunca devem ocorrer. Como conseqüência, este equipamento irá transmitir sempre que desejar, podendo ser esta a causa de uma taxa elevada de colisões.

Procedimento **10.3**

Como o lado *full duplex* irá transmitir sempre que desejar, sem verificar se o meio está ou não ocupado, uma transmissão pode ser iniciada pelo lado *full duplex* quando o lado *half duplex* já tiver transmitido mais que 512 bits de um quadro. Isto caracteriza uma colisão tardia. Portanto, descasamento de modo de operação pode ser a causa de colisões tardias.

4.3.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verificar modo de operação e velocidade configurados para o enlace com problema;

Teste confirmatório 1

A forma mais simples de se confirmar o descasamento de modo ou velocidade de operação é verificar a configuração dos equipamentos ligados ao enlace suspeito. A interface de gerência de comutadores Cisco, por exemplo, oferece o seguinte comando:

```
comutador> show port [módulo[/porta]]
```

A saída deste comando mostra, dentre outras informações, os erros detectados, o modo e a velocidade de operação.

Pode-se também verificar o modo e a velocidade de operação de uma interface usando SNMP. A variável dot3StatsDuplexStatus da MIB Ether-Like [RFC2665] informa o modo de operação de uma interface e ifSpeed do grupo Interfaces da MIB-II [RFC2233] a velocidade de operação.

Quando placas de rede estão envolvidas pode ser mais complicado confirmar o descasamento. Algumas placas de rede podem ser configuradas manualmente para diversas velocidades e modos de operação. Outras sempre utilizarão a detecção automática. No Windows, por exemplo, através do gerenciador de dispositivos, você pode ver propriedades avançadas da placa de rede. Nelas você encontrará o modo e a velocidade de operação da placa de rede.

4.3.5 Sugestões de tratamento

Se for confirmado o descasamento de modo de operação ou velocidade devido a erros de configuração manual, a solução imediata é corrigir a velocidade ou o modo de operação das interfaces envolvidas. Para um melhor desempenho, sempre que possível use modo de operação *full duplex*. Se repetidores estiverem envolvidos, o modo de operação sempre deve ser *half duplex,* pois um repetidor não trabalha no modo *full duplex*.

Em comutadores Cisco os seguintes comandos deverão ser utilizados para solucionar o problema [CISCO-AUTO-NEGOTIATION]:

```
show port capabilities [módulo[/porta]]
set port speed [módulo[/porta]] {4 | 10 | 16 | 100 |
auto}
show port [módulo[/porta]]
set port duplex [módulo[/porta]] { full | half }
```

Por exemplo, para configurar a porta 1/1 como sendo 100 Mbps, *full duplex* execute:

```
comutador> (enable) set port speed 1/1 100
```

```
comutador> (enable) set port duplex 1/1 full
```

Tratando-se de máquinas com sistema operacional Windows, o modo e a velocidade de operação podem ser configurados, quando a placa de rede assim permitir[13]. No gerenciados de dispositivos do Windows, clique com o botão direito sobre a placa de rede que deve ser configurada. Escolha o item Propriedades. Na tabela Avançado você poderá modificar o modo e a velocidade de operação da placa de rede. Na Figura 4-6 a placa de rede está sendo configurada para o modo de auto-configuração.

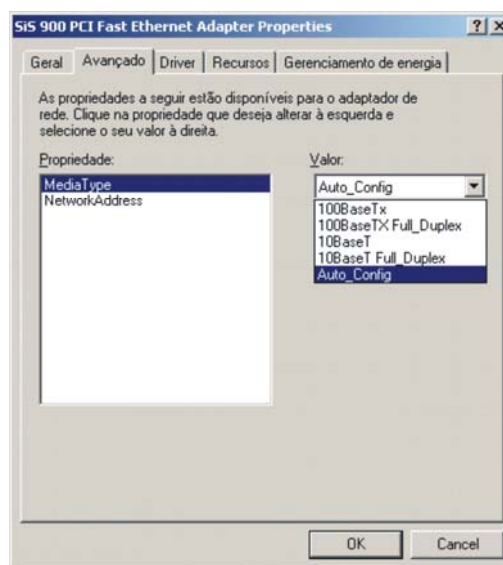



Figura 4-6: Propriedades avançadas da placa de rede SiS 900 em uma máquina com sistema operacional Windows.

Quando o descasamento for provocado por falha na negociação automática desconectar o cabo e conectá-lo novamente vai provocar uma nova negociação e pode ser que a nova negociação seja bem sucedida. Se este problema estiver ocorrendo com freqüência é aconselhável que você configure as interfaces envolvidas manualmente.

O comportamento *default* das portas dos comutadores é, geralmente, a negociação automática, quando esta funcionalidade é suportada. No entanto, uma boa prática de gerência é programar manualmente o modo e a velocidade de operação das portas que estarão ligadas a equipamentos fixos (com pouca probabilidade de serem trocados), como por exemplo servidores e roteadores. Esta prática elimina qualquer problema de negociação automática que possa vir a ocorrer e assegura que o gerente da rede sempre sabe em que modo e velocidade as portas estão operando. Esta prática assegura também que o melhor nível de desempenho possível será escolhido (já que cabe ao gerente definir o modo e a velocidade de operação).

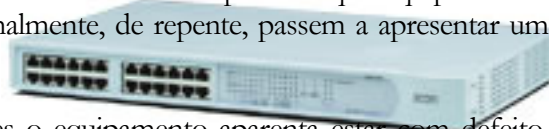
Encontrar enlaces sem comunicação é fácil. No entanto, descobrir enlaces que operam numa velocidade menor que a desejada já é bem mais complexo. Por

[13] Algumas placas de redes só podem ser configuradas para a negociação automática.

isso, todo cuidado é necessário, principalmente quando se trata de enlaces vitais para a satisfação dos usuários da rede.

4.4 Equipamento de interconexão defeituoso

4.4.1 Descrição

Equipamentos de interconexão podem deixar de realizar sua tarefa e não mais ser capaz de interconectar dispositivos de rede. É possível que equipamentos que costumavam funcionar normalmente, de repente, passem a apresentar um comportamento anormal.

A boa notícia é que muitas vezes o equipamento aparenta estar com defeito, mas uma reinicialização restabelece sua operação normal. Estas instabilidades podem ser causadas, por exemplo, por quedas rápidas de energia ou erros de programação do sistema operacional do equipamento.

No Brasil, o fornecimento de energia costuma ser de péssima qualidade, com oscilações que realmente podem causar danos aos equipamentos da rede. Portanto, uma checagem da rede elétrica da organização e das fontes de alimentação de energia dos equipamentos deve ser realizada com certa freqüência. É aconselhável também que os equipamentos mais críticos sejam alimentados por *no-breaks* de boa qualidade, de preferência *no-breaks online* senoidais.

A má notícia é que outras vezes o problema é mesmo no *hardware* do equipamento, nos seus *chips* de controle, sendo necessária a reposição dos elementos defeituosos.

Na prática, é difícil listar todas as possíveis causas de defeitos em equipamentos de interconexão. Eles chegam, muitas vezes, a passar a impressão de que têm um tempo de vida útil, após o qual começam a apresentar comportamentos indesejáveis.

O problema de equipamentos com portas defeituosas é reportado no problema **PLACA DE REDE OU PORTA DE EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSAS**.

4.4.2 Sintomas

Um equipamento de interconexão ou algumas de suas portas com defeito podem ser a causa de rede lenta ou falta de conectividade. Quanto mais próximo do *backbone* central estiver o equipamento, mais usuários serão afetados.

4.4.3 Sinais

Procedimento
10.4

Equipamento não operacional. Infelizmente não podemos tratar este sinal como um sinal diferencial. No procedimento 10.3 consideramos que um equipamento não está operacional se a comunicação com ele não for possível. Portanto, a causa de um equipamento não estar operacional pode ser realmente defeito no equipamento, mas pode ser outra que não envolva o equipamento. Por exemplo, um cabo de rede rompido.

Procedimento
10.5

Interfaces apresentam estado não operacional. Quando o estado administrativo de uma interface está configurado para que ela seja operacional, mas ela não funciona, certamente existe algum problema. Em especial quando um grupo de interfaces falha, desconfie não apenas de problemas nas interfaces, mas no próprio equipamento de interconexão.

Para se ter uma idéia relativa de quão saudável está o seu equipamento de interconexão, você pode medir a utilização de seus recursos [PERF&FAULT-CISCO]. Limiares de utilização de recursos sendo excedidos podem ser indicativos de falhas no equipamento.

Procedimento
10.6

Taxa elevada de utilização de CPU. Em geral, utilização média de CPU superior a 75% já deve ser investigada.

Procedimento
10.7

Taxa elevada de utilização de memória. Se a utilização de memória do equipamento está diferente da utilização habitual, é sinal de que algo diferente está ocorrendo. Em roteadores, o limiar de advertência para utilização de memória é 75%. Em hospedeiros deve-se medir não a utilização de memória em si, mas a freqüência de *page out*. Neste caso, veja procedimento 10.8

Procedimento
10.9

Tráfego alto de broadcast/multicast. Este tipo de tráfego pode ser gerado por um equipamento de interconexão defeituoso. O efeito negativo de um tráfego alto de broadcast/multicast é a saturação dos processadores dos equipamentos da rede.

4.4.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1 — Analisar LEDs;

TESTE 2 — Verificar configuração e estado do equipamento;

TESTE 3 — Testar sistema de transmissão do equipamento;

TESTE 4 — Substituir o equipamento sob suspeita;

Se durante a realização de um dos testes a seguir, algum comportamento anormal for verificado, reinicialize o equipamento e realize o teste confirmatório novamente.

Teste confirmatório 1

Analise os LEDs do equipamento suspeito. Os manuais dos equipamentos sempre trazem dicas de como analisar esses LEDs. Por exemplo, o manual pode informar que o LED *status* sempre deve estar aceso na cor verde. Se ele ficar piscando e apresentar alaranjada, é sinal de que muitos quadros/pacotes estão sendo descartados devido a erros, ou se ficar vermelho é sinal de que existe um problema grave no equipamento, etc. Pode acontecer de o problema ser confirmado através desta análise, mas é possível que equipamentos de rede se tornem defeituosos e seus LEDs não indiquem problema algum.

Teste confirmatório 2

Analise o equipamento sob suspeita. Verifique a temperatura do equipamento, se os ventiladores estão funcionando, se o fornecimento de energia está adequado, há quanto tempo o equipamento não foi reiniciado. Você pode fazer isto utilizando um terminal de gerência ou `telnet`. O manual do seu equipamento informa que comandos lhe darão estas informações.

Se o equipamento sob suspeita for um repetidor não gerenciável isto não será possível, mas por outro lado sua substituição é muito fácil e, se ao substituí-lo os sinais e sintomas cessarem, o defeito foi confirmado.

Em roteadores Cisco mais novos os comandos a seguir podem ajudar

```
roteador# show version
```

```
roteador# show environment all
```

O estudo do padrão de tráfego de cada interface do equipamento sob suspeita (unicast/broadcast/multicast) também pode auxiliar na confirmação do problema. Tráfegos de entrada e saída anormais (por exemplo, tráfegos de entrada e saída idênticos) podem ser indicativos da existência de um problema no equipamento.

Se você encontrou muitos limiares excedidos, temperatura fora do normal, fornecimento de energia inadequado, por exemplo, estabilizadores queimados, você está bem perto de confirmar o problema.

Em se tratando de equipamentos que operam além da camada física (comutadores e roteadores) o erro pode estar sendo causado por erro de configuração do equipamento, em especial se ele foi reconfigurado ou inserido há pouco tempo na rede.

Para realizar o teste a seguir será necessário ter em mãos uma máquina com placa de rede e um cabo de redes sem defeito. A máquina e o cabo de teste serão conectados a uma ou mais portas dos equipamentos suspeitos. Lembre-se, portanto, de configurar a rede nesta máquina adequadamente. Não apenas endereço IP e rota *default*, mas também modo e velocidade de operação para evitar o descasamento. Utilizando o cabo e a máquina de teste efetue o seguinte teste confirmatório:

Teste confirmatório 3

É possível que o equipamento esteja bem, mas uma ou mais interfaces estejam com defeito. Para testar as interfaces do equipamento veja os testes confirmatórios do problema **PLACA DE REDE OU PORTA DE EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSAS**.

A partir da máquina de teste, utilizando a ferramenta `ping`, deve-se tentar alcançar outros dispositivos da rede. Realize este teste conectado a máquina de teste em diversas portas do equipamento sob suspeita e enviando `ping` para outras máquinas da rede. Este teste serve para verificar se o equipamento está repassando os dados que recebe da forma correta, sem inserir erros.

Se dados não foram perdidos, os tempos de respostas foram satisfatórios e você conseguiu retorno de todas as máquinas para as quais enviou `ping`, é bastante provável que o equipamento não esteja com defeito.

Teste confirmatório 4

Se factível, substitua o equipamento sob suspeita por outro que esteja funcionando adequadamente. Será necessário configurar o novo equipamento corretamente, para que ele realize sua tarefa de interconexão como esperado. Use o *baseline*[14] de configuração da

[14] Leia mais sobre linha base de configuração na seção Sugestões de tratamento do problema VLANs não estão configuradas.

rede para realizar esta tarefa. Se os sinais e sintomas cessarem o equipamento estava realmente com defeito.

4.4.5 Sugestões de tratamento

Muitas vezes, solucionamos problemas em equipamentos simplesmente reiniciando-os. Se após a reinicialização o problema persistir a sugestão é estudar os manuais do equipamento em busca de dicas para este problema ou entrar em contanto com a assistência técnica especializada.

Problemas em equipamentos de rede que requeiram sua reinicialização não devem ser observados freqüentemente para o mesmo equipamento. Se, por exemplo, toda semana um certo comutador da empresa precisa ser reinicializado, uma investigação mais profunda deve ser iniciada. Comece investigando o sistema elétrico e de refrigeração do prédio. Se isso acontece muito raramente – 1 ou 2 vezes por ano – não há com o que se preocupar.

É aconselhável ter sempre equipamentos de reserva (repetidores, comutadores, roteadores, conversores, etc.) para substituir equipamentos danificados enquanto são consertados. Neste momento, a documentação da rede e a linha base de configuração são de grande auxílio, pois nelas encontram-se as descrições de como cada equipamento deve estar configurado e como eles se conectam aos demais dispositivos da rede.

Recomenda-se também que os gerentes da rede estejam sempre atentos em relação ao sistema operacional dos equipamentos da rede. De tempos em tempos os fabricantes lançam novas versões, que corrigem erros de programação das versões anteriores. Muitas vezes, portanto, um equipamento parece estar defeituoso, mas na verdade o erro está no seu sistema operacional. Além de erros que podem deixar o equipamento sem funcionar apropriadamente em determinadas condições, furos de segurança são constantemente descobertos, sendo também necessária a atualização do *software* e reforçando ainda mais a necessidade de se estar sempre atento às novas versões de sistemas operacionais que surgirem.

Uma excelente prática de gerência de configuração é organizar o que se chama de *baseline* – traduzido aqui como linha base – de configuração da rede. As configurações de dispositivos devem ser guardados em arquivos (que formam a linha base) de forma a:

- permitir que um ou mais dispositivos semelhantes sejam configurados a partir de um arquivo de *baseline* armazenado;
- verificar se a configuração da rede inteira está de acordo com o *baseline*;
- reconfigurar a rede parcial ou totalmente a partir do *baseline* em caso de problema.

A forma como a linha base vai ser salva em arquivos depende do modelo, fabricante e versão do sistema operacional do equipamento. Sempre que você

realizar alguma modificação no equipamento atualize o arquivo que guarda suas configurações.

Em comutadores Cisco Catalyst série 6000/6500 o seguinte comando pode ser utilizado:

```
console> (enable) copy config {tftp: | rcp:} [all]
```

Por exemplo, para salvar as configurações de comutador1 no servidor TFTP 192.168.101.10 o seguinte comando poderia ser executado:

```
Console> (enable) copy config tftp:comut1.cfg
IP address or name of remote host [192.168.101.10]? y
Upload configuration to tftp:comut1.cfg (y/n) [n]? y
.........
.........
.........
.
/
Configuration has been copied successfully. (10299 bytes).
Console> (enable)
```

Em roteadores Cisco com IOS versão 12.0 ou superior, use os seguintes comandos para armazenar em um arquivo a configuração completa do roteador:

```
roteador# copy system:running-config {tftp: | ftp: | rcp:}
```

Por exemplo, para salvar a configuração de roteador1 no servidor 192.168.101.10 use o comando a seguir:

```
roteador1# copy system:running-config tftp:
Remote host[]? 192.168.101.10
Name of configuration file to write [rtr1-confg]? <cr>
Write file rtr1-confg on host 192.168.101.10?[confirm] <cr>
![OK]
```

O comando `copy system` citado acima substitui o comando `write network` em roteadores com IOS mais antigos. O comando `write network` é válido para o IOS 12.0, mas em outros IOSs mais novos ele não mais existirá.

4.5 Placa de rede ou porta de equipamento de interconexão defeituosas

4.5.1 Descrição

Uma placa de rede é uma placa adicionada a um computador para permitir que ele se conecte à rede. Uma placa de rede que não está funcionando apropriadamente pode ser a causa de falta de conectividade ou de rede lenta.

Alguns exemplos de defeitos em placas de rede Ethernet são:

a placa não consegue ouvir a portadora (*carrier sense*) apropriadamente, causando um número excessivo de colisões, inclusive colisões tardias;

a placa começa a gerar quadros inúteis. Dentre os quadros inúteis gerados, coincidentemente, pode haver tráfego de *broadcast/multicast*, que, em excesso, satura os processadores dos equipamentos de rede que devem processar todos os quadros de *broadcast* recebidos e causa a lentidão da rede;

a placa gera quadros maiores que o indicado pelo padrão (1518 bytes).

Interfaces de equipamentos de interconexão (portas de repetidores, comutadores e roteadores) também podem apresentar defeitos e causar os mesmos sinais e sintomas de placas de rede defeituosas.

4.5.2 Sintomas

Os sintomas de placa de rede ou porta de equipamento defeituosos são: falta de conectividade ou rede lenta. Muitos usuários poderão ser afetados, depende da localização da interface defeituosa. Se esta interface fizer parte do *backbone*, muitos usuários serão afetados. Se for a interface de uma máquina cliente, apenas este reclamará.

4.5.3 Sinais

Procedimento **10.1**

Taxa elevada de erros, em especial erros de CRC e de alinhamento [GUIA-ETHERNET]. Idealmente, as taxas de erros de um enlace são muito próximas de zero. Em enlaces metálicos aceita-se no pior caso até 1 erro a cada 109 bits transmitidos e em enlaces óticos 1 erro a cada 1012 bits transmitidos.

Procedimento **10.2**

Taxa elevada de colisões. Uma taxa de colisões superior a 10% deve ser investigada.

Procedimento **10.3**

Placas de redes ou portas de equipamentos defeituosos também podem ser a causa de colisões tardias. As colisões tardias não são eventos normais da rede, e qualquer indício de colisões tardias deve ser investigado.

Procedimento **10.9**

Um tráfego alto de *broadcast/multicast* pode ser gerado por uma placa de rede ou porta de equipamento defeituosos. O efeito negativo de um tráfego alto de broadcast/multicast é a saturação dos processadores dos equipamentos da rede, além do aumento do consumo de largura de banda.

Procedimento **10.10**

Aumento da utilização do enlace. A interface de rede defeituosa pode gerar tráfego inútil. Este tráfego causará o aumento da utilização do enlace em relação à utilização normalmente observada.

Procedimento **10.11**

Existência de quadros maiores que o tamanho máximo imposto pelo padrão pode ser sinal de defeito em interfaces [GUIA-ETHERNET].

4.5.4 Testes confirmatórios

Este problema oferece sintomas e sinais muito semelhantes aos problemas de cabeamento. Se a probabilidade destes dois tipos de problema ocorrer é a mesma – nenhuma modificação foi feita na rede recentemente e nenhum destes problemas ocorreu proximamente – teste o cabo de rede antes de testar a interface. O teste da interface poderá falhar caso o cabo de rede esteja com problema.

RESUMO DOS TESTES

Para confirmar que uma placa de rede está com defeito realize um dos testes a seguir:

TESTE 1

Certificar-se de que o *driver* correto da placa de rede está devidamente instalado e a configuração do software de rede é apropriada;

TESTE 2

Substituir a placa suspeita por outra de teste;

TESTE 3

Substituir a máquina que abriga a placa suspeita por outra de teste;

Para confirmar o defeito em interfaces de equipamentos de interconexão:

TESTE 4

Troque a posição dos cabos nos equipamentos;

TESTE 5

Substitua o equipamento por outro;

TESTE 6

Teste as portas sob suspeita com `ping`;

Se você está desconfiado de uma placa de rede de um servidor ou estação cliente realize um dos três testes confirmatórios a seguir:

Teste confirmatório 1

Considere que o problema realmente está na placa de rede suspeita e tente solucioná-lo antes de confirmá-lo. Certifique-se de que o *driver* da placa de rede está corretamente instalado, que a configuração do *software* de rede é apropriada, que não está havendo conflitos de endereços de interrupção na máquina e, de preferência, realize também os testes contidos no disco de diagnóstico da placa suspeita – `diag` (veja a Seção **SUGESTÕES DE TRATAMENTO** para maiores detalhes). Os testes podem falhar, ou podem concluir que a placa estava mal instalada ou a rede mal configurada. Faça as devidas correções de acordo com o resultado de cada teste e verificação. Pode ser necessário reinstalar a placa ou reconfigurar o *software* de rede. Após as mudanças certifique-se de que o problema foi solucionado. Caso todos os testes indiquem que a placa está operando perfeitamente e ainda assim o problema

não foi resolvido, é bastante provável que a sua placa de rede esteja sem defeito e que o problema seja no cabo ou no equipamento conectado a ela.

Teste confirmatório 2

Troque a placa de rede suspeita por outra que esteja funcionando adequadamente. Se os sinais apresentados antes da troca ainda permanecerem, o problema não é com a placa. Se os sinais cessarem o problema de placa defeituosa foi confirmado.

Teste confirmatório 3

Se não for possível trocar a placa de rede por outra de teste, conecte o cabo que chega na placa de rede suspeita em uma máquina de teste e configure esta máquina com a mesma configuração de rede da máquina substituída. Se a máquina não possui endereço IP fixo e não conseguiu obter seu endereço através de um servidor DHCP ela estará sem endereço de rede. Neste caso, ,configure a máquina de teste com um endereço da rede à qual ela será conectada tomando o cuidado para não colocar um endereço IP em uso. Se os sinais e sintomas cessarem o problema é, certamente, na máquina substituída, seja na placa de rede ou no *driver* da placa. Se você não sabe se a taxa de erros do enlace ligado à interface suspeita está elevada, o problema pode ser também no servidor DHCP.

Se você desconfia de interfaces equipamentos de interconexão, realize um dos seguintes testes:

Teste confirmatório 4

Substitua o equipamento com porta sob suspeita por outro que certamente funcione, por exemplo, um equipamento de teste. A troca de um equipamento de interconexão por outro deve ser realizada com bastante cuidado. O equipamento de teste deve estar configurado de forma idêntica ao equipamento que será substituído. Caso contrário de nada valerá a substituição. Se após substituição do equipamento os sintomas e sinais cessaram, você confirmou que o equipamento está com problemas. Leve o

equipamento em questão para o seu laboratório e descubra se o defeito é no equipamento mesmo ou em uma de suas interfaces.

Teste confirmatório 5

Conecte o cabo de rede conectado à porta sob suspeita em outra porta que esteja funcionando apropriadamente. Se VLANs/roteadores estiverem envolvidos é necessário tomar cuidado com as configurações da rede. Se, com a troca, os sintomas e sinais cessarem, o problema foi confirmado.

Teste confirmatório 6

Para realizar este teste você necessitará de uma máquina e um cabo de testes. Conecte a máquina de teste com o cabo de teste em cada uma das portas do equipamento sob suspeita e tente alcançá-lo a partir da máquina de teste – com `ping`, por exemplo. Se o equipamento for um repetidor não gerenciável tente alcançar outro equipamento que também esteja conectado ao repetidor.

Se, ao conectar a máquina de teste em uma porta do dispositivo suspeito, o LED correspondente à porta não acender, é quase certa a existência de problema nesta porta (já que o cabo e a placa de rede utilizados são confiáveis). Se alguma porta do dispositivo estiver com defeito o mesmo não será alcançado através da porta ou será observada uma perda de pacotes elevada (o `ping` mostra a porcentagem de pacotes perdidos).

Suponha que você esteja desconfiado das interfaces de rede que ligam os equipamentos 10.16.253.254 e 10.16.254.33. Você então configura a sua máquina de testes adequadamente e a conecta na porta do equipamento 10.16.254.33 sob suspeita (as configurações de rede da máquina de testes devem ser semelhantes às configurações de rede da interface substituída). A partir da sua máquina de testes envie `ping` para o equipamento 10.16.254.33. Se o resultado do `ping` informou perda de quadros ou se nada foi retornado, e você tem certeza de que o equipamento está corretamente configurado, o problema foi confirmado.

Se você quiser, pode realizar este teste em outras portas do equipamento sob suspeita. Os tempos de resposta obtidos ao acessar o equipamento suspeito a partir de cada uma de suas portas devem ser praticamente os mesmos. Observe estes tempos de resposta ao receber as respostas dos `pings` em busca de comportamento anormal de alguma porta.

Se você não conseguiu confirmar a existência de interfaces de rede com defeito, outros problemas também de nível físico podem estar ocorrendo. Por exemplo: descasamento de velocidade ou modo de operação, cabo de rede danificado ou rompido ou ainda conectores defeituosos ou mal instalados.

4.5.5 Sugestões de tratamento

Se o sistema operacional utilizado for Windows, antes de trocar a placa remova o *driver* e o *software* de rede (geralmente TCP/IP) instalados e instale-os novamente. Verifique se o problema foi corrigido. Já aconteceu várias vezes de placas de redes em máquinas Windows simplesmente pararem de funcionar e após a reinstalação do *driver* e do *software* elas voltarem ao normal.

Verifique se a placa de rede está apropriadamente conectada ao *slot* PCI ou ISA da máquina A seguir, execute (novamente) os testes de diagnóstico da placa "com defeito" (geralmente chamam-se `diag`). Se os testes falharem a placa está realmente defeituosa. Caso contrário, remova e instale novamente o *driver* apropriado da placa de rede para o sistema operacional utilizado e reinstale também o *software* de rede.

Verifique se o *driver* instalado realmente corresponde à placa conectada ao computador. O computador terá que ser aberto para que se identifique que tipo de placa está conectada. Se for uma placa de rede embutida será necessário ter em mãos o manual da placa mãe da máquina e localizar o chip correspondente à placa de rede.

Se as sugestões anteriores não ajudaram a solucionar o problema troque a placa defeituosa por uma nova.

Se foi detectado que uma porta de um equipamento de interconexão está com defeito deve-se testar as demais portas do equipamento e o próprio equipamento antes de chamar a assistência técnica especializada. A substituição do equipamento com portas defeituosas por outro será necessária.

Se problemas como este em (placas de rede, portas de equipamentos e equipamentos de interconexão) ocorrem com certa freqüência é recomendado que se faça uma auditoria no sistema de alimentação de energia, pois é comum que estes problemas ocorram devido a instalações elétricas de má qualidade.

4.6 Interferência no cabo

4.6.1 Descrição

O sinal transmitido através do cabo pode sofrer interferências indesejáveis e ser corrompido durante a transmissão. As duas fontes mais comuns de ruído são Interferência Eletromagnética (EMI) e Interferência de Freqüência de Rádio (RFI). Fontes comuns de EMI são motores, lâmpadas florescentes e linhas de energia de corrente alternada. Exemplos de fontes de RFI são telefones celulares, rádio e TV [FIELD_TEST].

Cabos de fibra ótica são imunes a interferência e cabos de par trançado, felizmente, são também muito resistentes a estes tipos de ruído. Portanto, este é um problema pouco comum. Devido a esta forte resistência a ruídos os próprios padrões de cabeamento, como por exemplo EIA/TIA 568A, não se preocupam em definir requisitos de medições de ruído [FIELD_TEST].

4.6.2 Sintomas

O principal sintoma é rede lenta. Se o cabo que está sofrendo interferência faz parte do *backbone* muitos usuários podem ser afetados.

4.6.3 Sinais

Procedimento
10.1

Taxa elevada de erros [HAUGDAHL]. A taxa de erros de um enlace deve ser muitíssimo próxima de zero. Num enlace de par trançado, por exemplo, a quantidade de erros não deve ultrapassar 1 erro a cada 109 bits transmitidos. Para enlaces óticos aceita-se 1 erro a cada 1012 bits transmitidos. O tipo de erro que deve ser investigado quando há a suspeita de interferência no cabo em enlaces Ethernet é o erro de CRC.

4.6.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Procure por possíveis fontes de interferência ao longo do cabo;

Infelizmente, mesmo testadores de cabo com capacidade de medir o ruído não são válidos [HAUGDAHL] para detectar interferência no cabo.

Teste confirmatório 1

Tente descobrir se existe, ao longo do cabo, algum elemento que possa estar causando a interferência. Lâmpadas fluorescentes, aparelhos de rádio. TV, ar condicionado e aspiradores de pó são exemplos de equipamentos que podem causar interferência no cabo. Uma vez localizado um elemento que possa estar causando a interferência, tente reproduzir o problema artificialmente. Desligue-o ou afaste-o do cabo e teste o cabo para ver se a taxa de erros diminuiu. Ligue o equipamento no seu local original e teste o cabo em busca da taxa de erros. Se ao desligar ou afastar o equipamento a taxa de erros diminuir, a interferência foi confirmada.

4.6.5 Sugestões de tratamento

Se o problema é realmente interferência a sugestão é instalar o cabo em um caminho diferente [HAUGDAHL] ou retirar a fonte de interferência de perto do cabo. Algumas fontes comuns de interferência são apresentadas na descrição do problema.

4.7 Saturação de banda em segmentos Ethernet compartilhados

4.7.1 Descrição

Leia mais sobre Ethernet no apêndice 1

Quando os equipamentos de uma rede Ethernet trabalham no modo de operação *half duplex*, o acesso ao meio é compartilhado. Isto que dizer que quando alguém fala, os demais devem ficar calados. Para proteger a integridade dos dados, antes de enviar quadros, as estações certificam-se de que a rede não está em uso. No entanto, é possível que dois elementos da rede verifiquem, ao mesmo tempo, que não há atividade na rede e iniciem, ambos, a transmissão. O resultado é uma colisão. A colisão é detectada pelas estações envolvidas, e após um certo tempo aleatório, elas retransmitem os dados. Se, na segunda tentativa de transmissão, ocorrer uma segunda colisão, o tempo médio de espera para retransmissão é dobrado e assim sucessivamente, a cada colisão.

Minimizar colisões é, desta forma, uma tarefa crucial no projeto e gerência de redes Ethernet. Apesar de colisões serem eventos normais em enlaces Ethernet *half duplex*, quando em excesso, começam a degradar o desempenho da rede.

Uma taxa de colisões elevada pode ser resultado da existência de muito tráfego no segmento compartilhado. Muitas máquinas ou aplicações que requerem muitas transmissões de dados compartilhando o mesmo meio resultam em uma grande disputa por ele. Quando domínios de colisões estão congestionados, o número de colisões aumenta, mais retransmissões são necessárias, aumentando ainda mais a disputa pelo barramento, num círculo vicioso.

Todos os equipamentos ligados a um repetidor fazem parte do mesmo domínio de colisões. Cada porta de um comutador ou roteador define um domínio de colisões. Desta forma, é bem mais comum que este problema ocorra quando existem repetidores ligados entre si, e muitas máquinas ligadas nestes repetidores, formando um grande domínio de colisões.

4.7.2 Sintomas

O principal sintoma de domínios de colisões congestionados é rede lenta. Todos os usuários conectados no domínio de colisões congestionado serão afetados. Se a rede só está lenta para alguns serviços é possível que os servidores estejam em domínios de colisões congestionados.

4.7.3 Sinais

Procedimento
10.2

Procedimento
10.10

Taxa de colisões elevada. Este é um dos sinais típicos de saturação de banda em segmentos Ethernet compartilhados. Taxas de colisões superiores a 10% devem ser investigadas.

Utilização de enlaces Ethernet compartilhados (*half duplex*) superior a 50% de sua capacidade. Para outras tecnologias onde não há compartilhamento ou enlaces Ethernet operando no modo *full duplex* a utilização pode chegar a 70% sem comprometer o desempenho do enlace.

4.7.4 Testes confirmatórios

Se o problema foi descoberto através de reclamações dos usuários você já deve ter descoberto se mais máquinas foram adicionadas recentemente no segmento sob suspeita ou novas aplicações foram instaladas. Além disso, já sabe se estas modificações coincidem com o momento em que a rede começou a ficar lenta.

Se apenas a equipe de gerência tiver autorização para realizar tais modificações, vocês têm controle sobre elas mesmo que o problema tenha sido percebido através do monitoramento da rede.

Se nenhuma nova aplicação foi instalada, nenhuma nova máquina foi adicionada, algum outro problema pode estar levando a um domínio de colisões congestionado. Uma placa de rede ou repetidor defeituosos, por exemplo, podem estar gerando dados inúteis causando a sobrecarga do segmento e tornando a rede lenta. Nestes casos, além de colisões serão percebidos também erros, em especial CRC e alinhamento.

RESUMO DOS TESTES

TESTE 1

Ver origem das colisões;

TESTE 2

Verificar o estado do domínio de colisões antes das modificações, se possível;

Teste confirmatório 1

Faça este teste conforme descrito na Seção 10.2.3. Ele só pode ser realizado com o auxílio de um analisador de protocolos. Se ele estiver instalado em um computador pessoal será necessária também uma placa de rede especial para que erros e colisões sejam vistas pela aplicação. Com ele, você pode descobrir que existe uma estação específica que sempre participa de colisões. Como o teste envolve análise de tráfego você pode descobrir também que uma estação é responsável por enviar muitos quadros com erros ou muito tráfego de broadcast/muticast. Em todos estes casos o problema de saturação de banda em enlace compartilhado foi confirmado. No entanto, ele está sendo causado por outro

problema, provavelmente uma placa de rede ou equipamento defeituosos. Solucione este problema e conseqüentemente o problema de saturação de banda será resolvido. Os problemas **EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSO** e **PLACA DE REDE OU PORTA DE EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSAS** podem lhe ajudar.

Caso você não encontre uma estação "culpada", e está observando utilização dos enlaces e taxas de colisões elevadas no domínio de colisões em questão, o problema de saturação de banda em enlaces compartilhados foi confirmado e precisa ser solucionado. Para tal, ainda com o analisador de protocolos, descubra se existe tráfego de uma determinada aplicação em excesso, que está causando a saturação.

Se você não possui um analisador de protocolos capaz de perceber erros e colisões, o teste a seguir pode ser realizado.

Teste confirmatório 2

Se novas máquinas tiverem sido adicionadas e/ou novas aplicações tiverem sido instaladas nas máquinas clientes, tente simular o ambiente anterior às modificações proibindo o uso da nova aplicação e/ou desligando as novas máquinas por alguns instantes enquanto você verifica se o sintoma de rede lenta ainda é percebido. Pode não ser possível realizar este teste. Por exemplo, o sistema operacional das máquinas pode ter sido trocado e neste caso seria impossível retornar à situação anterior.

É interessante comparar a utilização e a taxa de colisões do segmento com e sem as novas máquinas e/ou aplicações.

Se com o ambiente anterior os sintomas e sinais deste problema não forem mais percebidos, é possível que o problema de saturação de banda em enlaces compartilhados esteja ocorrendo. No entanto, não se pode descartar problemas em nível de aplicação (aplicações com erros gerando tráfego absurdo) ou equipamentos ou placas de redes defeituosas.

Se novos equipamentos foram inseridos e neste teste foram desligados, teste-os. Se for comprovado que todos os equipamentos que tiveram que ser desligados estão funcionando adequadamente, mas a taxa de colisões continua alta ao lado de uma elevada utilização do segmento, o problema de domínio de colisões congestionado foi confirmado.

4.7.5 Sugestões de tratamento

Ao projetar uma rede não coloque muitas estações em um único domínio de colisões. Para obter o melhor desempenho deve-se segmentar a rede em domínios de colisões múltiplos. Para redes 10Base-T e 100Base-TX, por exemplo, o número máximo aceitável de estações em um domínio de colisões é 1024. Para redes 10Base-2 e 10Base-5 este número cai para 30 e 100 respectivamente. No entanto, não é regra geral que a largura de banda dos enlaces só se tornem saturadas quando este número é atingido. É perfeitamente factível que com um número inferior de máquinas as larguras de bandas dos enlaces se tornem saturadas. Isto vai depender de quanto tráfego cada máquina está gerando.

Se for detectado que a largura de banda está saturada, é necessário re-projetar a rede e segmentá-la de forma mais apropriada para que o número de colisões diminua. Equipamentos de interconexão que operam além da camada física (comutadores e roteadores, por exemplo) separam domínios de colisões. Portanto, a segmentação de domínios de colisões deve ser feita inserindo comutadores ou roteadores na rede.

Se servidores fizerem parte de domínios de colisões congestionados o número de usuários afetados será igual ao número de clientes do servidor, e este número pode ser bem grande e envolver até mesmo pessoas de fora da organização. Portanto, uma boa prática é conectar servidores a comutadores, nunca a repetidores. Desta forma os servidores não precisarão disputar o barramento Ethernet com outros usuários para transmitir seus dados.

4.8 Tipo errado de cabo

4.8.1 Descrição

Dois tipos de erros em cabos de pares trançados são:

1. Utilizar categoria de cabo inadequada;

A tecnologia de rede local mais bem aceita no mundo é Ethernet. Com o surgimento de Fast Ethernet e Gigabit Ethernet, a migração das redes Ethernet para Fast ou Gigabit Ethernet é um passo natural da evolução da maioria das redes locais. Começa-se substituindo os comutadores antigos por comutadores 10/100 Mbps ou por comutadores que ofereçam algumas portas Ethernet e outras Fast Ethernet e substituindo os repetidores por comutadores (provavelmente os comutadores Ethernet substituídos). Além disso, são adquiridas placas de rede 10/100 Mbps para os servidores. Aos poucos parte da rede opera a 100 Mbps e parte da rede a 10 Mbps. Em geral, o *backbone* é o primeiro a migrar para a nova velocidade. Com o tempo, toda a rede passa a operar na nova velocidade.

Para que a migração seja completamente bem sucedida podem ser necessários alguns ajustes na estrutura de cabeamento, não apenas com relação às regras de cabeamento, mas também com relação à categoria dos cabos utilizados. O

padrão 100Base-TX requer cabos de categoria 5 ou superior ou IBM STP (*Shielded Twisted Pair*) para funcionar em seu mais alto nível de desempenho. A estratégia deste requisito é minimizar a quantidade de retransmissões de quadros causadas por uma alta taxa de erros de bits. Ao migrar a rede para Fast Ethernet deve-se, portanto, substituir os cabos por outros de categoria adequada (quando cabos de categoria 3 estiverem em uso[15]). Caso contrário, a rede poderá sofrer problemas de desempenho, pois os cabos de pares trançados categoria 3 não suportam taxas de transmissão maior que 10Mbps.

2. Utilizar cabos cruzados em vez de cabos paralelos ou vice versa;

Dois tipos de cabos de pares trançados são tipicamente utilizados em uma rede: cabos paralelos e cabos cruzados. A diferença entre eles está relacionada a como os condutores estão dispostos nos terminais metálicos do conector RJ-45 em cada extremidade do cabo. A Figura 4-4 (ver página 51) mostra como os condutores devem estar dispostos em ambas as extremidades de cabos paralelos e cruzados.

Um cabo paralelo é utilizado para conectar estações finais a um equipamento de interconexão e cabos cruzados são utilizados para conectar dois equipamentos de interconexão entre si ou duas máquinas entre si.

4.8.2 Sintomas

Quando cabos cruzados ou paralelos são utilizados para interconectar equipamentos da rede erroneamente, o sintoma é falta de conectividade.

Quando a categoria de cabo errada é utilizada o sintoma pode ser rede lenta ou falta de conectividade. O tamanho do cabo pode influenciar: cabos bem curtos podem causar rede lenta, enquanto cabos maiores levarão à falta de conectividade.

4.8.3 Sinais

Procedimento
10.1

Quando cabos de categoria inadequada são utilizados o principal sinal é uma taxa elevada de erros, em especial erros de alinhamento. Requisita-se a utilização de certas categorias de cabo para operar em alta velocidade para minimizar a quantidade de erros de bits em um canal. Deve-se sempre suspeitar de uma taxa de erros que não esteja muito próxima de zero.

4.8.4 Testes confirmatórios

RESUMO DOS TESTES

[15] No Brasil, em geral, não se chegou a aproveitar o cabeamento telefônico (categoria 3). O cabeamento inicial, na maioria das organizações já iniciou com categoria 5, não sendo este problema comum por aqui.

TESTE 1

Verificar LEDs dos equipamentos ligados ao cabo suspeito;

TESTE 2

Verificar com um testador de cabos ou visualmente se o cabo é paralelo ou cruzado;

TESTE 3

Verificar categoria do cabo;

Se o sintoma é falta de conectividade realize o seguinte teste:

Teste confirmatório 1

Diante da falta de conectividade localize os equipamentos aos quais o cabo sob suspeita está conectado e verifique os LEDs. Geralmente placas de rede e portas de repetidores e comutadores possuem LEDs que indicam se há ou não conectividade ponto-a-ponto. Se cabos cruzados estiverem sendo utilizados em vez de cabos paralelos (ou vice-versa) os LEDs dos equipamentos ligados ao cabo de tipo errado não acenderão.

Se os LEDs não acendem ao conectar o cabo de rede, realize o teste a seguir:

Teste confirmatório 2

Verifique o tipo de cabo utilizado (se é um cabo cruzado, ou um cabo paralelo). Cabos cruzados devem ser utilizados para a conexão máquina ⇔ máquina e entre equipamentos de interconexão (por exemplo, repetidor ⇔ repetidor, repetidor ⇔ comutador) quando não existe porta de inversão em pelo menos um dos equipamentos.

Diferenciar cabos cruzados de cabo paralelos observando a disposição dos condutores metálicos no conector é uma tarefa simples: se a fiação for idêntica em ambas as extremidades do cabo, você está diante de um cabo paralelo, se for diferente, você provavelmente possui um cabo cruzado.

O ideal é utilizar um testador de cabos, que indique o tipo de cabo e ainda realize testes para verificar se o cabo está com problemas.

Geralmente as portas dos repetidores/comutadores/roteadores são numeradas e a porta identificada pelo maior valor possui ao lado o rótulo *Uplink* ou *MDI/X* e um botão que pode ser pressionado para cruzar ou descruzar o sinal. Isto significa que, utilizando esta porta, um cabo não paralelo pode ser usado para interligar dois equipamentos de interconexão entre si. Para interligar dois repetidores com um cabo cruzado, por exemplo,

conecte o cabo na porta *uplink* de um repetidor e no outro repetidor utilize uma porta comum. Na Figura 4-7 é apresentada uma porta *MDI/X* de um repetidor.

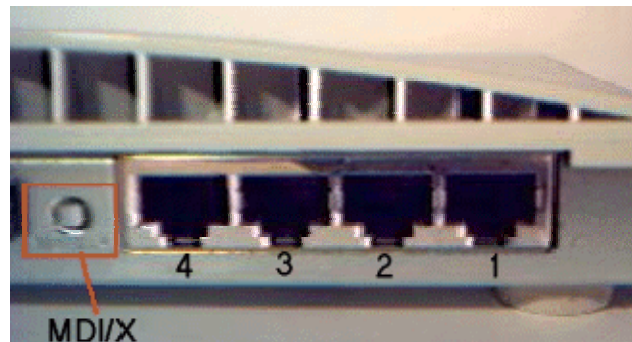



Figura 4-7: Porta de inversão de um repetidor.

Se você desconfia que cabos de categoria inadequada estão sendo utilizados, o teste a seguir deve ser realizado:

Teste confirmatório 3

Verifique se o cabo sob suspeita possui categoria inferior a 5 e está sendo utilizado para conectar equipamentos Fast Ethernet. É possível identificar cabos de categoria inferior a 5 sem a utilização de equipamentos de teste. Todos os cabos de categoria 5 possuem identificação gravada no próprio cabo pelo fabricante. Se o cabo sob suspeita não estiver identificado, este, com certeza, não é um cabo de categoria 5 ou superior. Se estiver marcado leia a identificação. Provavelmente ele será um cabo de categoria 5 ou superior. A Figura 4-8 apresenta a identificação de um cabo de categoria 5:.

Mais uma vez, o ideal mesmo é utilizar uma ferramenta para certificação do cabo suspeito. Verifique se ele pertence à categoria mínima indicada pelo padrão. Se ele não passar pelo teste o problema foi confirmado.

Figura 4-8: Marca no cabo de categoria 5.

4.8.5 Sugestões de tratamento

Troque o cabo errado por um tipo certo de cabo, confeccionado de acordo com o padrão. A Figura 4-4 (página 51) indica o padrão de cores para a confecção de cabos paralelos e cruzados de pares trançados.

Se cabos de categoria inadequada estão sendo utilizados, substitua-os por cabos de categoria 5 ou superior.

A força de uma corrente depende do seu elo mais fraco. Da mesma forma, o desempenho de um sistema de cabeamento é tão bom quanto o desempenho do seu enlace mais lento e a categoria de desempenho é correspondente à menor categoria encontrada nos componentes. Para evitar problemas de desempenho ao migrar para tecnologias de rede mais velozes, realize a certificação de seu cabeamento e assegure-se de que você possui um sistema categoria 5 ou superior.

4.9 Violação de regras de cabeamento Ethernet

4.9.1 Descrição

Leia mais sobre Ethernet no apêndice 1

Ao projetar uma rede Ethernet ou ao adicionar novos equipamentos a uma rede já em operação, algumas regras de cabeamento devem ser consideradas. As regras definem basicamente o comprimento máximo de cada segmento, o número máximo de segmentos entre duas estações finais e a quantidade máxima de estações finais em cada domínio de colisões. Como cada padrão Ethernet (por exemplo, 10Base-TX, 100Base-TX) opera em velocidade e/ou meio de transmissão diferentes, os valores máximos para cada uma das regras de cabeamento podem variar dependendo do padrão utilizado.

Seguir as regras de cabeamento impostas pelo padrão é de fundamental importância para que a rede tenha condições de oferecer o seu nível máximo de desempenho. Caso os padrões não sejam respeitados a rede continuará funcionando, porém com desempenho aquém do que lhe é permitido.

É mais freqüente que este problema seja causado por usuários. Em busca de uma nova conexão, um usuário simplesmente adiciona um repetidor em sua sala e não avisa aos responsáveis pela rede.

4.9.2 Sintomas

O principal sintoma da violação de regras de cabeamento é `rede lenta`. Entre as estações mais distantes pode haver falta de conectividade devido à atenuação do sinal.

4.9.3 Sinais

Procedimento
10.2

As regras de cabeamento informam o número máximo de estações em cada domínio de colisões. Quando esta regra é violada a principal conseqüência é uma taxa elevada de colisões, pois um número elevado de estações está competindo pelo meio. O problema, neste caso, é idêntico ao problema de saturação de banda em segmentos Ethernet compartilhados. Uma taxa de colisões superior a 10% deve ser investigada.

Procedimento
10.3

Ocorrência de colisões tardias. Este sinal existe quando são utilizados cabos com comprimento maior que o indicado pelas regras de cabeamento ou quando, entre duas estações finais, existem mais repetidores que o número máximo indicado. Em uma rede que segue as regras de cabeamento e cujos componentes não apresentam defeito a taxa de colisões tardias deve ser zero. Em outras palavras, qualquer índice de colisões tardias encontrado na rede indica um problema que deve ser investigado.

Procedimento
10.11

Uma outra conseqüência da utilização de cabos maiores que o sugerido pelo padrão é a atenuação do sinal (perda da força do sinal devido à resistência elétrica do meio de transmissão).

4.9.4 Testes confirmatórios

RESUMO DOS TESTES

Verificar o que está fora de especificação:

TESTE 1
- muitos repetidores entre estações, ou

TESTE 2
- cabo comprido demais.

Se a taxa de utilização também está alta, é mais provável que exista um número muito grande de estações finais em um domínio de colisões. Esta disputa acirrada pelo meio irá levar a uma taxa elevada de colisões. Este tipo de violação leva à saturação da banda em segmentos Ethernet compartilhados. Portanto, deve-se realizar os testes confirmatórios do problema **SATURAÇÃO DE BANDA EM SEGMENTOS ETHERNET COMPARTILHADOS**.

Os testes a seguir devem ser realizados se: 1) colisões tardias estiverem ocorrendo na rede, 2) existir a suspeita de que cabos muito compridos estão sendo utilizados, ou 3) desconfia-se que o número de repetidores entre duas estações finais não condiz com as regras de cabeamento.

Se uma estação de gerência indica a ocorrência de colisões tardias é muito provável que o cabeamento esteja fora de especificação, mas pode existir uma placa ou equipamento de rede defeituosos. Certifique-se de que o número máximo de repetidores entre duas estações finais do domínio de colisões está de acordo com as regras.

Teste confirmatório 1

Descubra qual o número máximo de repetidores entre duas estações finais do segmento. Quanto melhor documentada for a rede, mais simples, rápido e seguro serão a maioria dos testes. Se nenhuma documentação existe deve-se verificar fisicamente como é a topologia do domínio de colisões sob suspeita. Aproveite o trabalho e comece a documentar a sua rede. Se foi verificado que existem mais repetidores que o número máximo especificado entre duas estações finais, o problema de violação do padrão foi confirmado.

Infelizmente, os usuários mais ousados podem inserir novos equipamentos na rede sem que a equipe de gerência tome conhecimento.A documentação da rede lhe mostrará violações causadas pela equipe de gerência, mas não exclui a possibilidade de um usuário ter inserido um repetidor na rede para adicionar uma nova máquina em sua sala. Portanto, você terá que realizar uma investigação para descobrir se isto ocorreu.

Para verificar se existe algum cabo com comprimento maior que o máximo indicado no padrão deve-se utilizar um testador de cabos.

Teste confirmatório 2

Um testados de cabos TDR é capaz de indicar o comprimento de um cabo metálico (par trançado, por exemplo). Para obter o comprimento de cabos de fibras óticas use um OTDR. Mais informações sobre estes testadores podem ser encontradas no teste confirmatório 3 do problema **CABO ROMPIDO OU DANIFICADO**. Aproveite o testador não apenas para verificar o comprimento do cabo, mas para realizar um teste completo no cabo. Assim, você estará também excluindo ou confirmando a possibilidade problemas nos cabos e nos conectores.

Se algum cabo muito comprido for encontrado, o problema de violação de regras de cabeamento está confirmado. Não é preciso testar todos os cabos do domínio de colisões (exceto se está aproveitando a oportunidade para realizar a certificação do cabeamento). Os cabos sob maior suspeita são os cabos que foram adicionados mais recentemente.

Se nenhuma violação foi encontrada e colisões tardias ocorrem o problema é certamente em algum *hardware* da rede (placa de rede ou outro equipamento de interconexão) ou nos conectores.

4.9.5 Sugestões de tratamento

Projete sua rede novamente de modo a obedecer os padrões de cabeamento Ethernet. A nova solução deverá contar com repetidores que possuam um maior número de portas e/ou com mais comutadores e/ou roteadores.

Em uma rede Ethernet 10Base-TX, o número máximo de repetidores entre dois equipamentos de dados terminais que participam do mesmo domínio de colisões é 4. O comprimento máximo aceitável de cada cabo é 100 metros.

Já em uma rede 100Base-TX podem existir no máximo dois repetidores entre dois equipamentos terminais de dados. O comprimento máximo do cabo entre dois repetidores diretamente conectados não deve ultrapassar 205 m. O comprimento do cabo entre um repetidor e uma estação final é de no máximo 100 m.

Violações das regras de cabeamento são comuns quando a rede cresce aos poucos, principalmente com responsabilidade administrativa distribuída. Uma boa prática de gerência é manter manual ou automaticamente a documentação da topologia física da rede, onde repetidores e equipamentos terminais também sejam apresentados. Esta prática, além de ser útil na localização da maioria dos problemas de rede também pode evitar violações das regras de cabeamento. Manter essa documentação atualizada é muito difícil, e quase impossível quando se trata de redes muito grandes e muito dinâmicas. O descobrimento automático da topologia física da rede é implementado por algumas ferramentas de gerência, mas infelizmente, o descobrimento automático só detecta equipamentos gerenciáveis. Por isso, mesmo que ferramentas com descobrimento automático de topologia estejam sendo utilizadas, se existirem equipamentos não gerenciáveis na rede, deve-se ter o controle manual da documentação.

4.10 Referências

4.10.1 Livros

[GUIA-ETHERNET] Spurgeon, C. E. Ethernet – O Guia Definitivo. Tradução Daniel Vieira, Editora Campus, 2000.

[HAUGDAHL] Haugdahl, J. Scott. Network Analysis and Troubleshooting. Addison Wesley, 2000

[LAN WIRING] Trulove, J. LAN Wiring. McGraw-Hill, 1997.

[PERF&FAULT-CISCO] Maggiora, P. L. D., Elliot, C. E., Pavone Jr, R. L., Phelps, K. J., Thompson, J. M. Performance and Fault Management. Cisco Press. 2000.

4.10.2 Recursos online (Internet)

[BOURKE] Bourke, Tony. The Not-So-Usual Suspect.

http://www.hostingtech.com/nm/01_01_mismatch.html

[CABLETESTING-NEXT] Near End Crosstalk (NEXT).

http://www.cabletesting.com/CableTesting/Testing/Definitions/Definitions_NEXT.htm

[CISCO-AUTO-NEGOTIATION] Configuring and Troubleshooting Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation.

http://www.cisco.com/warp/public/473/3.html

[FIELD_TEST] An up-to-date review of physical layer measurements, cabling standards, troubleshooting practices and certification techniques.

http://www.wwtc.edu/nsf/AAMI_San_Jose/Arne_WebSite/cabling/cableTestingHandbook.pdf

[KREIBICH] Keibritch, Jay. Ethernet Auto-sensing: Adventures in manual configuration. Computing & Communications Services Office, Universidade de Illinois em Urbana-Champaign.

http://www-commeng.cso.uiuc.edu/docs/autosense/autosense.html

[STEINKE] Steinke, Steve. Troubleshooting Ethernet Problems.

http://www.networkmagazine.com/article/NMG20000724S0054

[TIPS-ETHERNET] Tips on Troubleshooting Ethernet Errors.

http://www.ncat.co.uk/Net_Lib/eth_errs.htm.

4.10.3 RFCs

[RFC2233] McCloghrie, K., F. Kastenholz. The Interfaces Group MIB using SMIv2. Novembro, 1997.

[RFC2665] Flick, J., Johnson, J. Definitions of Managed Objects for the Ethernet-like Interface Types. Agosto de 1999.

4.10.4 Livros base

[CISCO-INTERNETWORKING] Cisco Systems (Editor). Internetworking Technologies

Handbook. Cisco Press. Dezembro, 2000.

4.10.5 Outros recursos on-line

[CABLING_MISC] Misc. Cabling Information.

http://learn.wwtc.edu/aev/cabling/misc.htm

5 Problemas de nível de enlace

Neste capítulo encontram-se 5 problemas que podem ocorrer em uma rede relacionados à camada de enlace: Interface desabilitada, Problema com árvore de cobertura, Saturação de recursos devido a excesso de quadros de difusão, Tempo de envelhecimento de tabelas de endereços inadequado, Validade da cache ARP inadequada.

5.1 Interface desabilitada

5.1.1 Descrição

Com o auxílio de instrumentação adequada – uma estação de gerência SNMP ou um terminal de gerência, por exemplo – é possível desabilitar administrativamente uma interface de um equipamento de interconexão. Ao ser desabilitada administrativamente, uma interface fica inativa até que ela seja novamente habilitada.

É possível que os gerentes da rede desabilitem interfaces que não estão sendo utilizadas no momento para evitar que usuários realizem modificações topológicas sem o conhecimento da equipe de gerência. Ao desabilitar interfaces que não estão em uso você impede que usuários introduzam novas máquinas ou equipamentos de interconexão, por exemplo, ou passem a utilizar portas que não estão sendo monitoradas.

Por outro lado, essa prática pode gerar confusão. Por exemplo, o próprio gerente pode esquecer que as interfaces vagas estão desativadas. Ele pode adicionar novas máquinas e esquecer de habilitá-la. Talvez ele perca algum tempo tentando descobrir porque a rede não funciona para a nova máquina antes de se lembrar de habilitar a interface. Uma outra possibilidade é a de sua equipe de gerência ser alterada e os novos membros não saberem que as portas vagas estão desabilitadas. É um problema simples, mas quando a rede não está funcionando ninguém se lembra de olhar se a interface está ou não habilitada.

5.1.2 Sintomas

A interface desabilitada administrativamente ficará inativa e, portanto, o sintoma será falta de conectividade. Qualquer que seja o equipamento ligado à interface desativada não terá conectividade com outros membros da rede.

5.1.3 Sinais

Procedimento **10.10**

Inexistência de tráfego de saída e de entrada na interface. Em outras palavras, a utilização da interface desabilitada é zero.

Procedimento **10.13**

Interface administrativamente desabilitada. Ao verificar o estado da interface, percebe-se que ela foi desativada manualmente pela equipe de gerência da rede.

5.1.4 Testes confirmatórios

O sinal "interface administrativamente desabilitada" é diferencial Portanto, se ele for percebido o problema já está confirmado.

5.1.5 Sugestões de tratamento

Após descobrir que a interface está administrativamente desabilitada, decida se ela deve ser habilitada ou se houve uma mudança na rede e o cabo conectado a esta interface deve ser conectado a outra. Se a interface vai realmente ser utilizada, habilite-a via estação de gerência SNMP (reconfigurando a variável `ifAdminStatus`), através de um terminal de gerência conectado ao equipamento ou `telnet`.

Em comutadores Cisco, use os comandos a seguir para ativar e desativar operação de portas:

```
set port enable mod/port
set port disable mod/port
```

Se for decidido que as interfaces que não estão sendo utilizadas devem ficar administrativamente desabilitadas para evitar problemas, é recomendado que os cabos de rede estejam devidamente identificados, como descrito em [PERF&FAULT-CISCO], e que a documentação da rede seja suficiente para a detecção de mudanças realizadas por usuários. Por exemplo, a documentação da rede diz que as portas 6, 7 e 8 de um comutador não estão sendo utilizadas, mas ao observar o comutador o gerente vê que um cabo está conectado à porta 6. Leia mais sobre documentação de rede no apêndice 5 e em [PERF&FAULT CISCO].

Se os usuários se sentem confortáveis para constantemente modificar a topologia da rede sem o conhecimento dos gerentes, é recomendado restringir o acesso de usuários aos equipamentos. Colocá-los em um local onde apenas pessoas autorizadas possam entrar é uma boa medida.

5.2 Problema com árvore de cobertura

5.2.1 Descrição

Leia mais sobre o protocolo Árvore de Cobertura no capítulo 6

É comum que enlaces de redundância sejam criados entre comutadores para aumentar a confiabilidade da rede. Ao criar um enlace de redundância entre dois comutadores, o protocolo de árvore de cobertura (PAC) deve ser configurado e habilitado. Este protocolo tem por objetivo evitar que quadros enviados através da rede sejam transmitidos indefinidamente pelos comutadores que estão em laço.

Para realizar esta tarefa, o PAC define uma árvore que atravessa todos os comutadores da rede e força o bloqueio de enlaces de redundância para evitar os laços infinitos de quadros. Se um enlace que estava ativo se tornar indisponível, o PAC reconfigura a rede reativando enlaces antes bloqueados.

Abaixo são listadas algumas situações que podem levar ao laço infinito de quadros entre comutadores:

O PAC não está habilitado em todos os comutadores que participam do laço;

Os algoritmos de árvore de cobertura implementados pelos comutadores não são compatíveis entre si;

Os parâmetros configurados para a árvore de cobertura estão muito diferentes para cada comutador;

Existe um problema físico na rede que está causando perda ou atraso considerável de BPDUs (*Bridge Protocol Data Unit*) de configuração, causando a ativação de portas que deveriam estar bloqueadas;

Este último problema, na realidade, não é de árvore de cobertura. É um problema físico que causa a perda de quadros de controle da árvore de cobertura.

5.2.2 Sintomas

O laço infinito de quadros entre comutadores irá levar rapidamente à falta de conectividade.

5.2.3 Sinais

Procedimento **10.10**

Utilização de enlaces elevada. O laço infinito de quadros poderá levar à saturação da largura de banda dos enlaces. Será percebida uma utilização mais elevada que a utilização medida normalmente.

Procedimento **10.2**

Taxa de colisões elevada. A saturação da banda causará um aumento na taxa de colisões nas portas half duplex onde existe tráfego de entrada e de saída. Uma taxa de colisões superior a 10% deve ser investigada.

Procedimento **10.9**

Além da saturação de banda, quadros de *difusão* em excesso irão causar tempestades de quadros de difusão, e poderão saturar também os processadores dos equipamentos de interconexão e hospedeiros envolvidos. Durante uma tempestade de quadros de difusão, numa rede com velocidade de 10 Mbps, as máquinas ligadas aos comutadores em paralelo receberão alguns milhares de quadros por segundo. Numa rede que opera a 100 Mbps este número cresce para algumas dezenas de milhares de quadros de difusão por segundo. Os equipamentos mais novos de rede são capazes de processar uns 3000 quadros de difusão por segundo sem degradar seu desempenho. O problema saturação de recursos devido a tempestades de difusão traz mais informações sobre as conseqüências deste sinal.

Procedimento **10.6**

Utilização elevada de CPU. Tempestades de quadros de difusão podem causar nos equipamentos envolvidos (que recebem os quadros de difusão) altas taxas de utilização de CPU. Taxas de CPU acima de 90% são alarmantes e devem ser investigadas.

Procedimento **10.14**

Quando um comutador ainda não souber para qual de suas portas um quadro deve ser transmitido (a máquina destino ainda não se comunicou através deste comutador durante um certo tempo), ele enviará o quadro para todas as suas portas (enchente). Isto levará a uma tempestade de enchente. As tempestades de enchentes poderão levar à saturação da largura de banda dos enlaces e dos barramentos (*backplane*) dos equipamentos de rede envolvidos.

Alguns comutadores possuem a funcionalidade de proteger a rede contra tempestades de quadros de difusão e enchentes (supressão de quadros de difusão e enchentes). Após alcançar um certo limiar configurável – por exemplo, durante 1 segundo no máximo 100 quadros de difusão poderão ser comutados – o tráfego de quadros de difusão é suprimido. Se bem configurado, a tempestade de quadros de difusão (ou de enchentes) não chegará a ocorrer. No caso em que a supressão estiver habilitada, será necessário verificar se o limiar não está sendo atingido com freqüência.

5.2.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1 — Verificar estado e configuração do PAC nos comutadores envolvidos;

TESTE 2 — Verificar o algoritmo de árvore de cobertura utilizado pelos comutadores;

TESTE 3 — Verificar diâmetro máximo da rede comutada;

TESTE 4 — Verificar o intervalo de tempo em que BPDUs de configuração são enviadas e se notificações de mudança de topologia estão ocorrendo com freqüência;

Os testes a seguir devem ser realizados em todos os comutadores da rede que participam do laço.

Teste confirmatório 1

Com um terminal de gerência ou através de `telnet`[16], verifique se o PAC está configurado e habilitado em todos os comutadores em questão. Se estiver desabilitado, é provável que exista um laço e que o problema seja confirmado.

A tempestade de quadros de difusão e enchente causam saturação de recursos nos equipamentos de rede envolvidos e em hospedeiros. Ao tentar analisar o PAC em um comutador é possível que ele não responda aos comandos de gerência (pois está com recursos como CPU, por exemplo, saturados). Neste caso, desconecte temporariamente o cabo de um dos enlaces de redundância. Se os sinais e sintomas cessarem o problema está praticamente confirmado.. Para ter a certeza de que o PAC está desabilitado, verifique a configuração deste protocolo no comutador.

Os comandos de verificação do PAC mudam dependendo do fabricante e do modelo do equipamento. Os manuais dos equipamentos informarão como esta verificação pode ser realizada. Em um comutador Cisco, por exemplo, o comando `show spantree` retorna informações de configuração do PAC e ainda se ele está ou não habilitado. Abaixo segue um exemplo da resposta a este comando quando a árvore de cobertura não está configurada:

```
Sw-bb-vendas> show spantree

Spanning tree disabled
```

Se o PAC estiver habilitado o retorno seria semelhante ao exemplo abaixo:

```
Sw-bb-vendas> show spantree

Spanning tree enabled

Designated Root               00-50-1c-7a-8b-2e

Designated Root Priority      32768

Designated Root Cost          0

Designated Root Port          1/0
```

[16] Pode ser que a largura de banda dos enlaces esteja saturada e você não consiga chegar no equipamento através de `telnet`

```
Root Max Age   20 sec        Hello Time    2sec

Forward Delay  10 sec

Port,Vlan  Vlan  Port-State  Cost  Priority  Fast-Start  Group-method
--------   ----  ----------  ----  -------   --------   ------

1/1        1   forwarding  10        32  disabled

2/1        1   blocking    10        48  disabled

3/1        1   forwarding  10        32  enabled

4/1        1   forwarding  10        32  enabled

5/1        1   forwarding  10        32  disabled

6/1        1   forwarding  10        32  disabled

7/1        1   forwarding  10        32  disabled

8/1        1   forwarding  10        32  disabled
```

Além habilitar o PAC em todos os comutadores envolvidos, recomenda-se que eles também estejam configurados com os mesmos valores para cada um dos parâmetros de configuração do protocolo (*hello time*, *max age* e *forward delay*).

As informações sobre o PAC em um comutador podem também ser recuperadas através de uma estação de gerência SNMP. O grupo `dot1dStp` da MIB *Bridge* [RFC1493] traz informações sobre o PAC e é geralmente implementado pelos comutadores que suportam este protocolo. Pode não ser possível recuperar estas informações através da rede quando um problema com PAC estiver ocorrendo, uma vez que o sintoma é falta de conectividade. As variáveis dot1dStpHelloTime, dot1dStpForwardDelay e dot1dStpMaxAge informam os valores utilizados no momento pelo comutador para o *hello time*, *forward delay* e *max age* respectivamente. Além destas variáveis pode-se obter o estado e outras informações sobre as portas de cada comutador através da tabela `dot1dStpPortTable`.

Os valores de *hello time*, *max age* e *forward delay* configurados para o comutador (e que serão utilizados quando o comutador for a raiz da árvore) são encontrados respectivamente em: dot1dStpBridgeHelloTime, dot1dStpBridgeMaxAge e dot1dStpBridgeForwardDelay.

Na Seção **SUGESTÕES DE TRATAMENTO** são dados valores típicos para estes parâmetros do PAC.

Teste confirmatório 2

Problemas também podem surgir quando algoritmos de árvore de cobertura distintos estiverem sendo utilizados pelos comutadores.

Protocolos diferentes lidam de forma diferente com as BPDUs, podendo causar laços. Verifique em cada comutador que algoritmo de árvore de cobertura está sendo utilizado. É provável que esta informação seja encontrada nos manuais do comutador. Se mais de um algoritmo for encontrado o laço pode estar sendo causado por este descasamento. Os algoritmos implementados são o DEC e o IEEE, sendo este último mais utilizado.

Esta informação pode também ser recuperada através de uma estação de gerência SNMP. A variável dot1dStpProtocolSpecification da MIB *Bridge* informa que algoritmo de árvore de cobertura está sendo utilizado pelo comutador. Se o seu valor for 1 o algoritmo é desconhecido, se for 2 o algoritmo é o DEC e sendo 3 o algoritmo implementado pelo comutador é o IEEE.

Teste confirmatório 3

Outro parâmetro que deve ser investigado é o diâmetro da rede comutada, isto é, deve-se verificar o número máximo de comutadores entre duas estações finais da rede comutada. Para que o PAC opere corretamente o diâmetro da rede deve ser limitado. O IEEE recomenda um diâmetro máximo de 7 comutadores. Mais informações podem ser obtidas no padrão IEEE 802.1D, onde o PAC é definido.

É possível que todos os sinais/sintomas de um laço estejam sendo verificados, apesar de o PAC estar habilitado em todos os comutadores envolvidos. Na prática, a maioria dos problemas físicos levam a uma árvore de cobertura instável. Por exemplo, BPDUs de configuração podem ser perdidas devido a um cabo danificado, cabos com interferência, conectores mal instalados, largura de banda compartilhada saturada ou equipamento defeituoso, gerando a transmissão infinita de quadros na rede. Na realidade todos os problemas que possam causar a perda ou atraso elevado de dados (e conseqüentemente perda e atraso de BPDUs de configuração) podem levar o comutador secundário a entrar no estado de aprendizagem e mais tarde no estado *forwarding*, causando os laços, pois na realidade a raiz principal ainda está em funcionamento.

Se a raiz da árvore de cobertura, por exemplo, estiver muito ocupada, as BPDUs de configuração podem ser enviadas em intervalos bem maiores que o *hello time* configurado e causar o desbloqueio de portas que deveriam estar bloqueadas.

Para entender melhor o comportamento do PAC em sua rede comutada realize o seguinte teste com o auxílio de um analisador de protocolos ou uma estação de gerência SNMP:

Teste confirmatório 4

Conecte um analisador de protocolos em um comutador que participa da árvore de cobertura. Capture quadros BPDUs durante alguns minutos. Para capturar apenas os quadros BPDUs defina um filtro que aceite tudo que tenha como origem ou destino o grupo *bridge* (endereço físico 0180C2000000). Após a captura verifique se:

1. as BPDUs de configuração estão sendo enviadas no intervalo configurado (*hello time*) → os analisadores de protocolos geralmente informam o tempo que se passou entre a chegada de dois quadros consecutivos capturados. As BPDUs de configuração devem ser enviadas em intervalos regulares, definidos pelo *hello time*. Verifique de quanto em quanto tempo BPDUs de configuração são enviadas e compare este valor com o *hello time* configurado nos comutadores;

2. mudanças de topologia freqüentes (*Topology Change Notification* BPDU) estão ocorrendo → uma BPDU de mudança de topologia é enviada quando um novo equipamento/hospedeiro é adicionado à rede, quando um equipamento já conectado é ligado ou desligado, ou ainda quando há mudança de topologia física na rede (uma máquina estava ligada na porta 1 passou a ser ligada na porta 2, por exemplo). Se nenhuma destas situações está ocorrendo, uma BPDU de configuração não é enviada. Se for encontrado o número elevado de BPDUs de mudança de topologia em uma rede, aliado a um atraso significativo de BPDUs de configuração e nenhum dos testes anteriores acusou um problema de PAC, é possível que um problema físico esteja ocorrendo na rede;

Pode-se também provocar uma mudança (trocar a porta à qual uma máquina estava conectada) e verificar se BPDUs de mudança de topologia são realmente transmitidas.

É possível verificar se mudanças de topologia constantes estão ocorrendo com o auxílio de uma estação de gerência SNMP. A variável dot1dStpTimeSinceTopologyChange da MIB *Bridge* indica há quanto tempo (em centésimos de segundo) uma

notificação de modificação de topologia foi feita. Estude o comportamento desta variável durante algum tempo – 1h, por exemplo. Durante este tempo, certifique-se de que máquinas não estejam sendo inseridas ou retiradas (desligadas, por exemplo) da rede. Se for constatado um crescimento constante da variável dot1dStpTimeSinceTopologyChange, algum problema está realmente ocorrendo.

Se este último teste revelou que BPDUs de configuração estão sendo enviadas em intervalos muito maiores que o *hello time* configurado (com alguns segundos de atraso, por exemplo), ou mudanças constantes de topologia são notificadas quando teoricamente não deveriam ser, é possível que algum problema físico na rede esteja causando a instabilidade da árvore de cobertura, resultando em laços na rede.

5.2.5 Sugestões de tratamento

Se foi confirmado que alguns comutadores não estavam com PAC habilitado, configure-o e habilite-o. Em alguns comutadores o PAC já vem habilitado com a configuração *default*. No entanto, esta não é uma regra geral. Se laços forem planejados é necessário verificar se o protocolo está realmente habilitado para evitar este problema.

Se foi confirmado que algoritmos de árvore de cobertura incompatíveis estavam sendo utilizados, trate de reconfigurar os comutadores para apenas um algoritmo seja utilizado em todos eles.

Se os parâmetros de árvore de cobertura configurados em cada comutador são muito diferentes entre si modifique-os. Recomenda-se que os valores de *max age*, *forward delay* e *hello time* sejam idênticos para todos os comutadores que participam da árvore, pois isto evitará configurações problemáticas. A tabela abaixo apresenta os valores recomendados em [IEEE802.1D] para os parâmetros do PAC referenciados acima.

Parâmetro	Valor recomendado	Variação permitida
Bridge Hello Time	2.0	1.0 – 10.0
Bridge Max Age	20.0	6.0 – 40.0
Bridge Forward Delay	15.0	4.0 – 30.0

Tabela 5-1: Valores recomendados para alguns parâmetros do PAC.

Com os parâmetros *default* a árvore de cobertura irá funcionar, mas pode-se modificar certos parâmetros para certificar-se de que, por exemplo, a raiz e a raiz secundária são comutadores conhecidos, centrais e não sobrecarregados e portas mais velozes têm custos menores que portas mais lentas. Estas configurações podem ser realizadas com o auxílio de um terminal de gerência ou com auxílio do SNMP. Para alterar a prioridade de um comutador ou o custo de suas portas:

- através da interface de linha de comando com o auxílio de `telnet` ou um terminal de gerência → em cada equipamento comandos diferentes deverão ser executados para configurar o PAC. Em um comutador Cisco Catalyst 6000 a prioridade do comutador pode ser modificada com o comando `set spantree priority`. Veja mais informações sobre como proceder no manual do seu equipamento;

- utilizando SNMP e a MIB *Bridge* → ao modificar o valor da variável dot1dStpPriority da MIB *Bridge* modifica-se a prioridade do comutador. A variável dot1dStpPortPathCost da tabela dot1dStpPortTable pode ser alterada para se alterar o custo das portas do comutador.

5.3 Saturação de recursos devido a excesso de quadros de difusão

5.3.1 Descrição

Um quadro de difusão é endereçado a todas as estações que participam do mesmo domínio de difusão do emitente. Muitos protocolos de rede e aplicações em uma rede local dependem do envio de quadros de difusão para funcionar apropriadamente. Por exemplo: ARP, DHCP e NETBIOS.

Os domínios de difusão são limitados por roteadores e VLANs. Comutadores (onde VLANs não estão configuradas) não separam domínios de difusão e, portanto, transmitem um quadro de difusão recebido para todas as suas portas.

Uma tempestade de quadros de difusão ocorre quando um número elevado de quadros de difusão está trafegando na rede (milhares de quadros de difusão por segundo). Em um domínio de difusão, quanto maior o número de estações e a quantidade de protocolos e aplicações que dependem do envio de quadros de difusão, maior a quantidade desses quadros e maior a probabilidade da ocorrência de tempestades de quadros de difusão.

Tempestades de quadros de difusão podem ser causadas não apenas por excesso de máquinas ou de tráfego de difusão em um domínio de difusão, mas também devido a erros tais como:

- problema com protocolo árvore de cobertura (ver página 84);

- tempo de envelhecimento da cache ARP muito pequena em muitas máquinas da rede (ver página 96)

- defeitos em equipamentos e placas de rede (ver páginas 56 e 61);

- aplicações com erro de programação.

5.3.2 Sintomas

É mais comum que o excesso de quadros de difusão tornem a rede lenta. No entanto, dependendo da quantidade destes quadros, os usuários podem reclamar de falta de conectividade.

5.3.3 Sinais

Procedimento **10.9**

Quantidade excessiva tráfego de quadros de difusão. Tipicamente, uma máquina envia em média um quadro de difusão a cada 10 segundos. Em um domínio de difusão com 1600 máquinas, por exemplo, seria normal um tráfego de difusão em torno de 160 quadros por segundo. Quando este número cresce para milhares de quadros de difusão por segundo, uma tempestade de quadros de difusão está ocorrendo. Os processadores de equipamentos mais modernos conseguem processar alguns milhares de quadros de difusão por segundo sem comprometer o desempenho da rede.

Alguns comutadores possuem a funcionalidade de suprimir o tráfego de difusão. Eles podem ser configurados para aceitar até uma certa quantidade de quadros de difusão por segundo (limiar), e descartar os demais quadros. Neste caso, deve-se observar se o limiar estabelecido está sendo constantemente alcançado.

Procedimento **10.6**

Utilização alta de CPU. Uma quantidade excessiva de quadros de difusão trafegando na rede pode saturar os processadores de equipamentos de interconexão e hospedeiros. Durante tempestades de quadros de difusão intensas, a utilização de CPU dos equipamentos da rede irá crescer bastante em relação ao normal, e poderá chegar a alcançar 99/100%. Em geral, taxas médias de utilização de CPU superiores a 75% já devem ser investigadas.

Procedimento **10.10**

Aumento da utilização de enlaces. Tempestades de quadros de difusão aumentam a utilização dos enlaces que participam do domínio de difusão onde a tempestade está ocorrendo. Será observado um aumento da utilização dos enlaces em relação ao tráfego normal da rede. Considerando quadros de difusão de 64 Kbps, se 1000 quadros de difusão trafegam a rede por segundo, a largura de banda consumida por eles é: 1000 x 64 x 8 = 512 Kbps.

5.3.4 Testes confirmatórios

O sinal quantidade excessiva de tráfego de difusão é diferencial. Se alguns milhares de quadros de difusão estão trafegando na rede por segundo, a tempestade de quadros de difusão já foi confirmada.

Como citado anteriormente, tempestades de quadros de difusão podem ter várias causas. Dentre elas encontram-se: problemas com o protocolo árvore de cobertura, tempo de envelhecimento da *cache* ARP muito pequena, problemas de *hardware*, aplicações com erros de programação e ataques de negação de serviço. O teste descrito nesta Seção tem por objetivo auxiliar a encontrar a causa real do problema.

RESUMO DOS TESTES

TESTE 1

Examinar os tipos de quadros de difusão que estão trafegando e qual a sua origem;

Teste confirmatório 1

Quando uma tempestade de quadros de difusão estiver ocorrendo, capture os quadros de difusão da rede em questão com um analisador de protocolos. Dicas para a realização deste teste podem ser encontradas nos procedimentos 9.1 e 10.9. Após capturar os quadros decodifique-os e tente responder as seguintes questões:

1. os quadros de difusão são, em sua maioria, provenientes de alguma máquina específica ou são originários de diversas máquinas da rede?

2. qual o protocolo de nível superior dos quadros de difusão? Por exemplo, são todos (ou quase todos) ARP? Ou não há um protocolo de nível superior que se sobressaia em relação aos outros?

Se a maioria dos quadros vem de uma máquina específica da rede, a placa de rede desta máquina pode estar defeituosa. Veja o problema **PLACA DE REDE OU PORTA DE EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSAS** na página 61.

Se os quadros de difusão capturados, carregam quase sempre dados de um mesmo protocolo de camada superior ou aplicação, é provável que o problema seja na configuração do protocolo, ou erros de programação de aplicações.

Quando o mesmo quadro de difusão trafega na rede indefinidamente, o problema é com o protocolo árvore de cobertura. Veja **PROBLEMA COM ÁRVORE DE COBERTURA** na página 84.

Se não foi possível encontrar um padrão, isto é, os quadros de difusão vêm das mais diversas origens e carregam dados de diversos protocolos, é bem provável que o domínio de difusão esteja super povoado.

5.3.5 Sugestões de tratamento

Se foi confirmada a existência de tempestades de quadros de difusão na rede devido a um domínio de difusão congestionado, deve-se quebrar o domínio de

colisões em vários domínios menores configurando VLANs nos comutadores ou inserindo roteadores na rede.

5.4 Tempo de envelhecimento de tabelas de endereços inadequado

5.4.1 Descrição

Leia mais sobre comutadores no apêndice 4

Um comutador mantém uma tabela, chamada tabela de endereços, que informa através de qual de suas portas uma máquina (identificada pelo seu endereço físico) pode ser alcançada. Esta tabela inicia-se vazia, e à medida que as máquinas se comunicam através do comutador, ela vai sendo povoada, através de uma técnica chamada *backward learning*[17].

Cada entrada na tabela de endereços informa a porta que dá acesso a uma certa máquina da rede. Quando o comutador recebe um quadro de uma máquina, a entrada correspondente na tabela de endereços é atualizada. Se uma maquina da rede não se comunica através do comutador durante um certo tempo (chamado tempo de envelhecimento), a entrada na tabela de endereços correspondente à máquina em questão é removida.

Ao receber um quadro destinado a um certo endereço físico, o comutador procura em sua tabela de endereços através de que porta o quadro deve ser enviado. Se não encontrar esta informação na tabela de endereços, o quadro é enviado para todas as portas do comutador (*flooding*, traduzido aqui como enchente).

Em uma rede comutada com muitas máquinas, quando o tempo de envelhecimento configurado em um comutador for muito pequeno, enchentes serão realizadas com bastante freqüência, gastando largura de banda da rede desnecessariamente.

Por outro lado, quando o tempo de envelhecimento for muito grande e o protocolo Árvore de Cobertura não estiver ativado, entradas na tabela de endereços podem se tornar obsoletas. Como conseqüência, máquinas podem ficar incomunicáveis por um certo período de tempo, até que a tabela de endereços seja ajustada. A tabela de endereços é ajustada quando a máquina que sofreu modificação se comunica através do comutador, ou quando acaba o tempo de envelhecimento.

Quando o protocolo de Árvore de Cobertura estiver habilitado, BPDUs de mudança de topologia serão enviadas sempre que alguma mudança ocorrer na rede. Sendo assim, em redes totalmente comutadas, mesmo que o tempo de

[17] Ao receber um quadro através de uma de suas portas, emitido por uma máquina origem A, o comutador aprende através de que porta a máquina A pode ser alcançada, e adiciona esta informação na sua tabela de endereços.

envelhecimento esteja grande[18], a tabela de endereços será rapidamente atualizada.

5.4.2 Sintomas

Quando os comutadores estiverem configurados com tempo de envelhecimento muito pequeno, os usuários poderão reclamar de rede lenta. Se o tempo de envelhecimento estiver muito grande, o sintoma será conectividade intermitente.

5.4.3 Sinais

Procedimento **10.14**

Quando o tempo de envelhecimento for muito pequeno, o sintoma principal será ocorrência muito freqüente de enchentes. As enchentes podem ser verificadas visualmente (através dos LEDs do comutador), da mesma forma como ser verificam tempestade de quadros de difusão. Quase todos os LEDs acendem de um vez, indicando que um quadro foi enviado por enchente ou difusão.

Procedimento **10.10**

Em grande quantidade, as enchentes irão causar o aumento da utilização dos enlaces em relação à utilização normalmente verificada.

5.4.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verificar valor configurado para tempo de envelhecimento de tabelas de endereço;

Teste confirmatório 1

Pode-se verificar o valor do tempo de envelhecimento da tabela de endereços de um comutador com o auxílio de uma estação de gerência SNMP. A variável dot1AgingTime da MIB *Bridge* [RFC1493] informa o período de validade dos endereços em segundos (um valor entre 10s e 10^6s). Esta variável pode ser utilizada para recuperar o valor da validade e também para configurar um novo valor.

---

18 Se existirem repetidores ligados aos comutadores e uma máquina for transferida de um repetidor para outro, mesmo que o PAC esteja habilitado a atualização da tabela de endereços não será imediata.

Pode-se também verificar e atualizar o tempo de envelhecimento com o auxílio de um terminal de gerência ou de `telnet`. Os comandos a serem executados dependem do modelo e do fabricante do equipamento. Em um comutador Cisco série 6000, por exemplo, o tempo de envelhecimento pode ser configurado/recuperado da seguinte forma com os comandos:

```
show cam agingtime [vlan]
```

```
set cam agingtime [vlan] <aging_time_em_segs>
```

Por exemplo, para configurar um tempo de envelhecimento de 5 minutos na VLAN 1, o seguinte comando deve ser executado:

```
console> (enable) set cam agingtime 1 300
```

5.4.5 Sugestões de tratamento

Este problema não ocorre comumente. Para ele vir a afetar a rede, é necessário que existam milhares de máquinas numa rede comutada, onde os comutadores estão configurados com tempo de envelhecimento muito pequeno (algumas poucas dezenas de segundos), ou, que mudanças sejam muito freqüentes e o tempo de envelhecimento configurado esteja muito alto.

O tempo de envelhecimento recomendado no padrão IEEE 802.3D é `300 segundos`, isto é, 5 minutos, sendo este o valor *default* do tempo de envelhecimento na maioria dos equipamentos.

5.5 Validade da cache ARP inadequada

5.5.1 Descrição

Leia mais sobre ARP no apêndice 7

Em redes TCP/IP, o protocolo ARP é utilizado para mapear endereços lógicos em endereços físicos. ARP é usado apenas em redes que suportem envio de quadros de difusão, como por exemplo, Ethernet. Todos os endereços mais recentemente mapeados são armazenados temporariamente em uma tabela, chamada cache ARP. O funcionamento do protocolo de resolução de endereços é simples: quando uma estação deseja encontrar o endereço físico correspondente a um determinado IP ela procura em sua cache ARP. Se o mapeamento desejado não for encontrado na cache ARP, a estação envia um quadro de difusão ARP, solicitando à estação com o IP em questão que informe seu endereço físico.

Cada entrada da cache ARP é válida durante um certo tempo, chamado tempo de validade da cache ARP. Se o tempo de validade da cache ARP for muito longo e houver mudanças na rede, a cache conterá informações incorretas e quadros poderão ser encaminhados para o destino errado. As mudanças que

podem levar a uma cache ARP incorreta são: troca de placa de rede de equipamentos, substituição de um equipamento por outro com mesma configuração IP e modificação de endereço IP de equipamentos. Além disso, se o serviço DHCP estiver sendo utilizado, uma máquina cliente pode ter um certo endereço IP em um dia e no dia seguinte outro endereço IP. Portanto, após o vencimento do tempo de validade da cache ARP, as entradas desta tabela expiram.

Se o período de validade da cache ARP for muito pequeno, muitos quadros de difusão ARP estarão trafegando na rede, consumindo recursos de equipamentos de interconexão e hospedeiros e podendo tornar a rede lenta.

Não é comum que o problema com tempo de validade de cache ARP ocorra. Os sistemas operacionais vêm com valores *default* para o tempo de validade da cache ARP. Este problema só ocorrerá se estes valores forem modificados para outros valores inadequados em alguma estação de trabalho.

5.5.2 Sintomas

Quando o período de validade for muito pequeno, os usuários podem sentir a rede lenta. Muitos quadros de difusão estarão trafegando na rede, pois um mapeamento deve ocorrer sempre (ou quase sempre) que duas máquinas desejam se comunicar.

Em máquinas onde o período de validade for muito grande, os usuários poderão sentir falta de conectividade durante determinado período de tempo com outras máquinas quando houver mudanças na rede. Por exemplo, na cache ARP de uma máquina, o endereço IP 10.10.10.1 é mapeado para 4445.5354.ab00. Esta entrada ficará válida durante algumas horas. No entanto, a placa de rede de 10.10.10.1 apresentou problemas e teve que ser substituída. Até que o tempo de validade da cache ARP vença, esta máquina não poderá se comunicar com a máquina 10.10.10.1.

5.5.3 Sinais

Procedimento **10.15**

Se o período de validade da cache ARP for muito pequeno, uma quantidade excessiva de quadros de difusão ARP poderá estar trafegando na rede. Em geral, o número de quadros de difusão ARP por segundo é bem menor que o número de máquinas no mesmo domínio de difusão.

Procedimento **10.10**

Como conseqüência do sinal anterior, poderá ser observado um sutil aumento na utilização dos enlaces que fazem parte do domínio de difusão, uma vez que o número de quadros de difusão ARP enviados aumenta. Quadros de difusão ARP são pequenos, por isso o aumento da utilização dos enlaces pode ser imperceptível.

5.5.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Descobrir estações que estão gerando muitos quadros ARP;

TESTE 2

Verificar valor configurado para tempo de validade da cache ARP nas máquinas suspeitas;

Quando o sintoma for falta de conectividade temporária com algumas máquinas, um ou mais usuários irão reclamar. Realize o teste confirmatório 2 nas máquinas envolvidas. Quando o sintoma for rede lenta, e houver suspeita de que o tempo de validade da cache ARP está muito pequeno, realize o teste confirmatório 1 antes de realizar o teste confirmatório 2.

Teste confirmatório 1

No procedimento ANALISANDO TRÁFEGO DE DIFUSÃO ARP (Seção USANDO UM ANALISADOR DE PROTOCOLOS) você encontrará dicas mais precisas de como realizar este teste. Com um analisador de protocolos capture os quadros ARP que trafegam na rede e tente responder a seguinte questão:

- existe uma ou mais máquinas que são responsáveis pelo envio da maioria dos quadros ARP que trafegam na rede, ou todas as máquinas, de forma mais ou menos homogênea, estão enviando quadros ARP?

Se for detectada que uma ou algumas poucas máquinas estão enviando muitos quadros ARP, verifique a validade da cache ARP configurada para estas máquinas. Caso contrário, é mais provável que exista um número muito grande de máquinas em um domínio de difusão, mas ainda é possível que todas as máquinas tenham tido seus tempo de validade da cache ARP alterados.

Para obter o tempo de validade da cache ARP, realize o teste confirmatório 2. Cada sistema operacional oferece um meio diferente para se configurar o tempo de validade da cache ARP. O teste abaixo considera apenas os sistemas operacionais Windows NT, Windows 2000 e Linux Slackware.

Teste confirmatório 2

No Windows NT/2000, use um editor de registro (`regedit.exe`) para procurar o valor do tempo de validade da cache ARP. No editor, procure os parâmetros de registro chamados ArpCacheLife e ArpCacheMinReferencedLife. Se estes

parâmetros existirem, verifique o valor estabelecido. Caso o parâmetro não exista, o valor *default* estará valendo, e não é provável que esteja ocorrendo algum problema com tempo de validade da cache ARP. Valores como alguns poucos segundos (1 segundo, por exemplo) ou milhares de segundos (12400 segundos) podem ser a causa do problema.

No Linux, procure no arquivo /usr/src/linux/net/ipv4/arp.c o valor estabelecido para base_reachable_time. Para entender melhor o código veja a definição de neigh_table e neigh_parms em /usr/src/linux/include/net/neighbours.h. O valor *default* é 30 segundos. Se um outro valor foi encontrado, esta modificação pode ser um problema se for um valor muito grande, ou muito pequeno.

Em comutadores Cisco série 6000 o comando abaixo lhe informará o tempo de validade da cache ARP do equipamento:

```
Console> (enable) show arp
```

Se os valores *default* forem configurados, e ainda assim os sinais/sintomas persistirem, o problema não é validade de cache ARP inadequada.

5.5.5 Sugestões de tratamento

Recomenda-se que o tempo de validade da cache ARP permaneça com o valor *default* implementado pelos fabricantes de sistemas operacionais. Abaixo encontram-se dicas de como modificar o valor do tempo de validade da cache ARP no Linux Slackware (núcleo 2.2.16) e no Windows NT e 2000.

No Linux, o tempo de validade é randômico, variando entre base_reachable_time/2 e 3*base_reachable_time/2. Modificando-se o valor de base_reachable_time em /usr/src/linux/net/ipv4/arp.c e recompilando o núcleo, modifica-se o tempo de validade da cache ARP. Em /usr/src/linux/include/net/neighbour.h estão definidas as estruturas neigh_table e arp_parms. Esta última contém parâmetros de configuração ARP, dentre eles o base_reachable_time. Baseado nas definições deste arquivo, pode-se encontrar mais facilmente o valor de base_reachable_time em arp.c.

No Windows NT e 2000, os parâmetros de registro chamados ArpCacheLife e ArpCacheMinReferencedLife são configurados com valores *default* durante a instalação do Windows. Quando ArpCacheLife não é modificado, entradas da cache ARP são removidas sempre que passarem 2 minutos sem serem utilizadas. O ArpCacheMinReferencedLife informa o tempo mínimo que uma entrada da cache ARP utilizada deve permanecer válida na cache, sendo 600 segundos (10 minutos) o valor *default*. Se estes parâmetros não forem encontrados do registro, significa que os valores *default* estão sendo utilizados. Para considerar novamente os valores *default*, exclua os parâmetros de sistema mencionados acima e reinicialize o sistema.

Em comutadores Cisco série 6000 use o comando abaixo para modificar o tempo de validade da cache ARP:

```
Console> (enable) set arp agingtime
<agingtime_em_segs>
```

5.6 Referências

5.6.1 Livros

[PERF&FAULT-CISCO] Maggiora, P. L. D., Elliot, C. E., Pavone Jr, R. L., Phelps, K. J., Thompson, J. M. Performance and Fault Management. Cisco Press. 2000.

5.6.2 Recursos online (Internet)

[CISCO-STP] Understanding Spanning-Tree Protocol. http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm

[IEEE802.1D] Padrão IEEE 802.1D. Part 3: Media Access Control (MAC) Bridges. http://standards.ieee.org/getieee802/download/802.1D-1998.pdf

5.6.3 RFCs

[RFC1493] Decker, E., Langille, P., Rijsinghani, A., McCloghrie, K. Definitions of Managed Objects for Bridges. Julho, 1993

5.6.4 Livros base

Comer, D. Internetworking with TCP/IP: Principles, Protocols, and Architectures. Volume 1. Quarta edição. Prentice Hall, 2000.

Cisco Systems (Editor). Internetworking Technologies Handbook. Cisco Press. Dezembro, 2000.

Tanenbaum, A. Computer Networks. Tercecira edição. Prentice Hall, 1996.

Capítulo

6

6 Problemas de nível de rede

Neste capítulo encontram-se 14 problemas que podem ocorrer em uma rede relacionados à camada de rede: Tabela de rotas de hospedeiros incorretas, Endereço IP de hospedeiro incorreto, Hospedeiro com máscara de rede incorreta, Cliente DNS mal configurado, Servidor DHCP mal configurado, Rotas estáticas mal configuradas, Equipamento inserido em VLAN incorreta, VLANs não estão configuradas, Comutadores não conseguem trocar informações sobre VLANs entre si, Ambiente RIP-1 com VLSM e/ou redes não contíguas, Diâmetro RIP com mais de 15 roteadores, Roteadores RIP-2 não enviam ou recebem pacotes RIP-1, Tráfego RIP saturando largura de banda, Filtro IP não permite a passagem de tráfego RIP (UDP 520).

6.1 Tabela de rotas de hospedeiros incorretas

6.1.1 Descrição

Seja estática ou dinamicamente, um roteador default deve ser configurado em hospedeiros. Quando o hospedeiro deseja se comunicar com outra máquina que não faz parte de sua rede local (não tem mesmo prefixo e máscara de rede que ele), os dados desta comunicação devem ser entregues ao roteador default.

Se o roteador *default* estiver sendo configurado manualmente, erros de digitação podem ocorrer e causar o problema. Pode-se ainda esquecer de configurar o roteador *default* de um hospedeiro, o que também é bastante problemático.

Se o roteador *default* estiver sendo configurado dinamicamente, através de um servidor DHCP, a configuração do escopo no servidor pode estar incorreta, causando o problema.

Se o hospedeiro puder se comunicar diretamente com mais de um roteador, a tabela de rotas do hospedeiro pode se tornar incompleta. Idealmente, deveríamos configurar o hospedeiro para usar o roteador que ofereça o melhor caminho para cada destino.

6.1.2 Sintomas

Quando a tabela de rotas de um hospedeiro estiver com rota *default* incorreta ou inexistente, a conseqüência para os usuários é que só haverá conectividade com máquinas da mesma sub-rede. Os usuários de máquinas com este

problema dirão que a rede só funciona internamente, que eles não conseguem navegar em *sites* fora da organização (ou do departamento). Um agravante pode ainda existir: se o servidor de nomes estiver em outra sub-rede, ele não será alcançável, e o usuário da máquina com erro não conseguirá nem mesmo se comunicar com máquinas da mesma sub-rede através dos nomes das máquinas.

6.1.3 Sinais

Procedimento

11.8

Se um hospedeiro estiver com a tabela de rotas incompleta, ele receberá do seu roteador *default* mensagens ICMP de redirecionamento. O roteador default envia essas mensagens para a máquina com tabela de rotas incompleta, para informá-la que existe um caminho melhor para certos destinos.

6.1.4 Testes confirmatórios

RESUMO DOS TESTES

Se a configuração for manual:

TESTE 1

Verifique o endereço IP do roteador *default* configurado;

Se a configuração do roteador *default* for dinâmica:

TESTE 2

Verifique a configuração do escopo em questão no servidor DHCP;

Se o escopo estiver correto:

TESTE 3

Verifique a configuração de cliente DHCP no hospedeiro;

Teste confirmatório 1

O cliente de um hospedeiro reclamou. Ele citou justamente os sintomas descritos anteriormente. Você está desconfiado que o roteador *default* está incorreto ou não foi configurado nesta máquina cliente. Olhe na documentação da rede qual o endereço do roteador *default* para a máquina em questão. Na própria máquina verifique qual o roteador *default* configurado. Dicas para realizar este teste podem ser encontradas no 11.13.

Se você observar que o endereço do roteador *default* está incorreto ou não existe ou ainda que a tabela de rotas do hospedeiro está incompleta, o problema foi confirmado.

Teste confirmatório 2

Este teste deve ser realizado se as máquinas com problema obtêm as configurações de rede através de um servidor DHCP.

Se o escopo do servidor DHCP estiver incorreto, todas as máquinas clientes apresentarão o mesmo erro – seja o endereço do roteador *default* incorreto, seja qualquer outro erro.

Verifique a configuração do escopo no servidor DHCP. Comumente, são definidos em um escopo: a faixa de endereços IPs a serem alocados aos clientes, o endereço IP do roteador *default*, a máscara de sub-rede e o endereço IP do servidor de nomes do domínio.

Para acessar o gerenciador do servidor DHCP em servidores Windows NT clique em: Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. No Windows 2000, no menu Iniciar escolha Programas > Ferramentas Administrativas > DHCP. Em ambos os sistemas operacionais surgirá um programa que serve de interface para a gerência do servidor DHCP. A interface destes programas é bem semelhante à interface do Windows Explorer. Navegue no painel esquerdo e no painel direito serão apresentadas as configurações do escopo DHCP correspondente.

No Linux Slackware verifique as configurações do servidor DHCP no arquivo /etc/dhcpd.conf. A opção `routers` define o endereço do roteador *default*.

Teste confirmatório 3

Veja nas máquinas clientes envolvidas se as configurações do protocolo TCP/IP foram obtidas dinamicamente ou não. No Windows NT, clique com o botão direito do mouse sobre o ícone Ambiente de Rede e escolha o item Propriedades. Escolha a tabela Protocolos, selecione o protocolo TCP/IP e pressione o botão Propriedades. Verifique se a máquina está configurada para obter um endereço IP automaticamente, ou se as configurações de rede são estáticas. Verifique também as configurações avançadas. Se é um servidor DHCP que vai oferecer todas as configurações de rede (incluindo roteador *default*, IP do servidor de nomes e máscara de rede) nenhuma configuração manual precisa ser feita.

No Linux Slackware as configurações das interfaces de rede localizam-se no arquivo /etc/rc.d/rc.intet1. Caso a máquina seja

cliente DHCP, neste arquivo não serão encontradas as configurações TCP/IP, mas sim a ativação do cliente DHCP.

Com este teste você pode descobrir máquinas que deveriam ser clientes DHCP, mas estão com configurações estáticas incorretas.

6.1.5 Sugestões de tratamento

Para solucionar o problema configure o roteador *default* corretamente. Se a configuração de rede do hospedeiro for manual, modifique a configuração do roteador manualmente.

No Windows isto é feito a partir do Painel de Controle de Rede. Este painel é obtido como descrito no teste confirmatório 3. Selecione o protocolo TCP/IP e clique no botão Propriedades. Uma janela, que permite configurar a rede TCP/IP aparecerá. Selecione a orelha Gateway e configure o endereço correto do roteador *default*.

Caso você tenha descoberto que o escopo DHCP está incorreto, será necessário corrigi-lo. Em servidores Windows NT clique em: Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. Clique com o mouse sobre o escopo desejado e no menu Escopo, selecione o item Propriedades. Para visualizar e modificar o endereço do roteador *default* escolha no menu Opções DHCP o item Escopo e verifique as configuração do roteador *default* (opção 003 router). Modifique o endereço do roteador *default* apropriadamente. Em seguida reinicie o servidor DHCP para que a nova configuração seja levada vista.

Em servidores Windows 2000, no menu Iniciar escolha Programas > Ferramentas Administrativas > DHCP. Abra a árvore correspondente ao escopo em questão (no painel esquerdo). Sobre o item Opções do Escopo clique com o botão direito do mouse. Surgirá um menu. Escolha o item Propriedades. Modifique a opção 003 Router para corrigir o problema. Por fim, reinicialize o servidor DHCP.

Em servidores DHCP Linux modifique o arquivo /etc/dhcpd.conf. Na linha que inicia com `option routers` corrija o endereço do roteador *default*. Em seguida também será necessário reiniciar o servidor DHCP:

```
# /etc/rc.d/init.d/dhcpd restart
```

Ou:

```
# kill –TERM <no. do processo dhcpd>[19]
# dhcpd
```

[19] Este número pode ser obtido com o comando `# ps –ae | grep dhcpd`.

6.2 Endereço IP de hospedeiro incorreto

6.2.1 Descrição

Primeira mente, vamos definir o que consideramos um endereço IP incorreto. Existem três situações:

- o prefixo de rede do endereço está incorreto. O endereço deveria ser 192.168.1.2 e na realidade foi configurado como 193.168.1.2;

- o endereço de rede de dois hospedeiros é igual, causando IPs duplicados na rede;

- esqueceram de configurar o endereço IP do hospedeiro – bastante incomum, mas possível.

As máquinas clientes que tiverem com endereço IP incorreto não conseguirão se comunicar corretamente na rede.

6.2.2 Sintomas

Se o endereço IP da máquina está incorreto o usuário da máquina reclamará de falta de conectividade. Veja um exemplo: a máquina pc-2, que deveria ter o endereço 19**2**.168.1.2, foi configurado com o endereço 19**3**.168.1.2. O endereço do roteador *default* é 192.168.1.254. Com estas informações, a tabela de rotas do hospedeiro é mais ou menos assim:

Rede destino	Máscara	Interface	Custo	End. do roteador
193.168.1.0	255.255.255.0	Eth0	1	193.168.1.2
0.0.0.0	0.0.0.0	Eth0	1	192.168.1.254

O que ocorrerá quando o usuário de pc-2 tentar usar o serviço que está na máquina 192.168.1.10? pc-2 pensa que esta será uma entrega indireta e que deve enviar os dados desta comunicação para o roteador *default*. No entanto, pc-2 fica isolado ao perceber que o roteador *default* também não faz parte da mesma rede local que ele. pc-2 simplesmente não saberá para quem enviará os dados. A comunicação entre pc-2 e 192.168.1.3 também não será possível. pc-2 acha que será uma entrega indireta. Enfim, nada funcionará.

Se o endereço IP da máquina estiver duplicado os usuários das máquinas com IP duplicado sentirão conectividade intermitente. Em sistemas operacionais mais novos (Windows ME e 2000, por exemplo) endereços IP duplicados são rapidamente detectados e as interfaces de redes envolvidas desativadas. Uma mensagem de erro é apresentada ao usuário informando que a interface foi desativada por ter detectado IP duplicado.

Clientes DHCP também detectam quando recebem do servidor um endereço IP duplicado e solicita-o outro endereço.

Quando pelo menos duas máquinas são configuradas com o mesmo endereço IP, a seguinte situação ocorrerá: nas *caches* ARP das outras máquinas que se

comunicam com a máquina em questão diretamente e dos roteadores, ora o endereço está apontando para o MAC de uma máquina, ora para o de outra.

Suponha, por exemplo, que ambos os usuários das máquinas com IP duplicado resolveram visitar um determinado *site* fora da organização. Ambas as máquinas usam o mesmo roteador *default*. Quando a primeira máquina falar com o roteador ficará registrado na cache ARP do roteador que determinado MAC corresponde ao IP duplicado. Imediatamente depois, quando a segunda máquina falar, a tabela ARP do roteador será modificada. Em seguida, um datagrama chega no roteador destinado à primeira máquina com IP duplicado que falou com o roteador, mas ele será entregue à segunda máquina, pois na *cache* ARP do roteador é o MAC da segunda máquina que está registrado.

Desta forma, os usuários das máquinas com IP duplicado ora conseguirão se comunicar através da rede, ora não.

6.2.3 Sinais

Procedimento **11.1**

Quando existem máquinas com mesmo IP na rede, serão encontradas pelo menos duas respostas à mesma requisição ARP. Isso ocorrerá porque todas as máquinas que possuem o mesmo IP responderão ao quadro de difusão ARP que requisita o endereço físico correspondente ao IP em questão.

Procedimento **11.12**

Quando máquinas forem configuradas com IP incorreto (erro de digitação, por exemplo) poderão ser encontrados na rede quadros de difusão enviados por máquinas de outra sub-rede. No domínio de difusão de pc-2, onde todas as máquinas possuem prefixo de rede 192.168.1, serão encontrados quadros de difusão enviados pela máquina 193.168.1.2.

6.2.4 Testes confirmatórios

Se você descobriu que existe mais de uma resposta à mesma consulta ARP já está confirmado que existem IPs duplicados em sua rede. Mesmo tendo confirmado o problema, caso exista mais de 1 servidor DHCP em sua rede, o teste confirmatório 2 pode ser aplicável ao seu caso. Caso este sinal diferencial não tenha sido percebido, realize o teste confirmatório 1.

RESUMO DOS TESTES

TESTE 1

Verifique o endereço IP configurado nas máquinas clientes;

Se você descobrir que existem IPs duplicados na rede:

TESTE 2

Se existir mais de um servidor DHCP na rede, certifique-se de que as faixas de endereços de cada um não se sobrepõem;

Teste confirmatório 1

Em muitos casos, o próprio sistema operacional detectará a duplicidade de endereços, estando o problema de IPs duplicados confirmado. Se você já verificou que existem duas respostas ARP à mesma requisição, o problema de IPs duplicados também já foi confirmado.

Se você desconfia que houve erro de digitação ao configurar o endereço IP de uma máquina cliente ou ele não foi configurado, será necessário verificar a configuração de rede desta máquina. Se ela for cliente DHCP veja se não há erros de configuração no escopo DHCP.

Em máquinas Windows use o programa `ipconfig` ou `winipcfg`. Eles lhe retornarão configurações de rede das máquinas, incluindo o endereço IP configurado.

Em máquinas Linux use o comando `ifconfig –a`. Este comando apresenta informações sobre todas as interfaces da máquina.

Teste confirmatório 2

Se existir mais de um servidor DHCP[20] na rede, assegure-se de que a faixa IP configurada em cada servidor é diferente, para evitar IPs duplicados na rede. Este teste, é dependente da implementação do servidor DHCP utilizada.

Para acessar o gerenciador do servidor DHCP no Windows NT clique em Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. Clique com o mouse sobre o escopo desejado e no menu Escopo, selecione o item Propriedades. Surgirá uma janela informando a faixa de endereços IPs configurada, a máscara de rede, os endereços reservados e o tempo de concessão escolhido.

No Windows 2000 clique em Iniciar > Programas > Ferramentas Administrativas > DHCP. Navegue no escopo em questão no item Pool de Endereços e verá os valores de cada item no painel à direita.

[20] No Windows 2000 é possível criar um cluster de servidores DHCP. Neste caso, este teste não é necessário.

No Linux, a faixa de endereços é definida no arquivo /etc/dhcpd.conf. Veja as linhas que começam com a palavra `range`.

6.2.5 Sugestões de Tratamento

Se você confirmou a existência de endereços IP duplicados na rede, reconfigure os endereços IP das máquinas envolvidas para que não mais apresentem endereços iguais ou incorretos.

Em máquinas Windows você deve entrar no Painel de Controle de Rede, escolher o tipo de rede TCP/IP e clicar no botão Propriedades. Modifique o endereço IP da máquina.

Em máquinas Linux Slackware você deverá modificar arquivo de inicialização rc. No Linux Slackware o arquivo /etc/rc.d/rc.inet1 contém as configurações da rede. Modifique o endereço IP das máquinas envolvidas (ou de pelo menos uma delas) para corrigir o problema.

No Red Hat – e nos sistemas Linux baseados no sistema de inicialização System V – modifique o arquivo de configuração da interface envolvida no problema (que está com IP duplicado). No diretório /etc/sysconfig/network-scripts existe um arquivo de configuração para cada interface da máquina. Os nomes destes arquivos começam sempre com `ifcfg-`, seguidos do nome do dispositivo. Se você deseja modificar o endereço IP da interface eth0, então edite o arquivo ifcfg-eth0 e modifique o endereço configurado na linha que se inicia com `IPADDR`.

Após modificar o endereço de rede de uma interface reinicialize[21] a máquina para que a nova configuração seja carregada e também para certificar-se de que as modificações corretas foram feitas e o problema foi resolvido.

Se o problema era no escopo DHCP, certifique-se de que endereços de máquinas servidoras (geralmente endereços fixos e muitas vezes configurados manualmente) não estão sendo fornecidos a clientes DHCP. Em máquinas Windows NT, por exemplo, clique em Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. Em seguida clique com o mouse sobre o escopo desejado e no menu Escopo, selecione o item Propriedades. Surgirá uma janela informando a faixa de endereços IPs configurada, a máscara de rede, os `endereços reservados` e o tempo de concessão escolhido. Veja se todos os endereços reservados estão corretamente configurados.

[21] No Windows, ao tentar fechar o Painel de Controle de Rede você ser4á automaticamente questionado se quer reiniciar a máquina.

6.3 Hospedeiro com máscara de rede incorreta

6.3.1 Descrição

Leia mais sobre máscaras de rede no apêndice 7

Máscaras de rede IP são número formados por 32 bits. A máscara de rede de um hospedeiro está incorreta quando:

- ela é maior do que deveria ser, ou
- menor do que a máscara correta.

Costuma-se representar máscaras de rede por quatro números decimais (entre 0 e 255) separados por um ponto (.).

Suponha, por exemplo, que a máscara de rede de pc-2 (128.128.10.2) deveria ser 255.255.254.0. Em bits este número é 11111111111111111111111000000000 (23 dígitos 1 seguidos de 9 dígitos 0). Suponha que por falta de atenção a máscara de pc-2 foi configurada para 255.255.255.0. Em bits esta máscara é: 11111111111111111111111100000000. Este é um número maior que a máscara correta apresentada anteriormente, não é? Pois bem, este é um exemplo de que você pode erroneamente configurar uma máscara de rede maior para seu hospedeiro. Devido a este erro, pc-2 acha que faz parte da rede local 129.128.10.0/255.255.255.0, quando na realidade pc-2 pode se comunicar diretamente com todas as máquinas da rede 128.128.10.0/255.255.255.0 (128.128.10-11.0). Quando pc-2 tentar falar com a máquina 128.128.11.2 vai tentar fazer uma entrega indireta, isto é, vai entregar os dados para o roteador *default*, quando na realidade uma entrega direta poderia ser realizada.

Máscaras de rede menores também podem ser configuradas por erro. Considere novamente pc-2, cuja máscara de rede correta é 255.255.254.0. Ao configurar pc-2 você, por descuido configurou a máscara de rede 255.255.0.0. Em bits, esta máscara é 11111111111111110000000000000000. Um número bem menor que a máscara correta! Neste caso, pc-2 tenta fazer entregas diretas a máquinas que não fazem parte de sua rede local. Por exemplo, pc-2 tentará fazer uma entrega direta à máquina 128.128.1.1.

6.3.2 Sintomas

Se a máscara de sub-rede de um hospedeiro está com o número de bits 1 menor que o correto, o usuário desta máquina sentirá falta seletiva de conectividade, pois não haverá conectividade para algumas redes. No exemplo acima, por exemplo, excetuando-se a rede 128.128.10.0/23 o usuário de pc-2 não conseguirá se comunicar com outras máquinas pertencentes à rede 128.128.0.0/16. A máquina com máscara incorreta tentará fazer uma entrega direta a estas máquinas e não conseguirá. O usuário, em gera; dirá que alguns serviços não estão funcionando. Se a comunicação com o servidor de nomes for impossibilitada devido ao erro, de máscara o usuário reclamará que a rede não funciona, já que a maioria dos serviços é acessada através dos nomes dos servidores.

Caso a máscara de rede esteja com um valor maior que o correto, tudo poderá funcionar bem, depende de quem é o roteador default. No exemplo de máscara com valor maior apresentado na seção anterior, pc-2 vai tentar fazer entregas indiretas a máquinas com prefixo de rede 128.128.11. Para tal, o roteador default será utilizado. Neste exemplo, o roteador default é alcançável, pois tem prefixo 128.128.10. Assim, nenhum sintoma seria percebido pelos usuários, mas alguns sinais seriam ainda percebidos pelo gerente. Mas, se o roteador default tivesse prefixo 128.128.11? O usuário da máquina não conseguiria se comunicar com quaisquer máquinas, exceto com máquinas com prefixo de rede 128.128.10. Portanto, quando a máscara de rede está configurada com um valor maior que o correto, o usuário da máquina poderá reclamar de falta de conectividade, ou que só consegue se comunicar com algumas máquinas da rede local.

6.3.3 Sinais

Procedimento **11.8**

Quando a máscara de sub-rede está configurada com um valor maior que o correto, várias mensagens ICMP REDIRECT serão encontradas na rede. O roteador default envia essas mensagens para a máquina com problema, para informá-la que ela poderia ter feito uma entrega direta.

Procedimento **11.13**

Além disso, poderão ser encontradas nas tabelas de rotas de hospedeiros com máscara maior que a máscara correta, rotas específicas para outros hospedeiros, e não apenas rotas para redes, como se espera. Essas rotas são aprendidas pelo hospedeiro através das mensagens ICMP REDIRECT mencionadas no sinal anterior.

Procedimento **11.2**

Quando a máscara de rede está com um valor menor que o valor correto, trafegarão na rede requisições ARP, sem a resposta correspondente. A máquina com máscara de rede incorreta pensa que máquinas de outras redes fazem parte de sua rede local e tentará fazer uma entrega direta.

6.3.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verifique a máscara do hospedeiro;

TESTE 2

Se a máscara é obtida através de um servidor DHCP verifique a configuração do escopo no servidor DHCP;

Teste confirmatório 1
Em máquinas Windows use o programa `ipconfig` ou `winipcfg`. Eles lhe retornarão configurações de rede das máquinas, incluindo a máscara de rede configurada.

Em máquinas Linux use o comando `ifconfig –a`. Este comando apresenta informações sobre todas as interfaces da máquina.

Se a máscara de rede configurada estiver incorreta o problema foi confirmado. Se esta máquina está obtendo suas configurações de rede dinamicamente através de um servidor DHCP, realize o teste confirmatório 2.

Teste confirmatório 2

Você descobriu que um ou mais clientes DHCP estão com máscara de rede incorreta. Verifique no servidor DHCP a configuração do escopo envolvido.

Em servidores Windows NT clique em: Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. Selecione o escopo desejado e no menu Escopo, selecione o item Propriedades. A máscara de rede configurada está correta?

Em servidores Windows 2000, no menu Iniciar escolha Programas > Ferramentas Administrativas > DHCP. Clique com o botão esquerdo do mouse sobre o escopo desejado e escolha o item Propriedades. A máscara de rede está correta?

Em servidores Linux veja a configuração DHCP no arquivo /etc/dhcpd.conf. A linha que inicia com `option subnet-mask` define a máscara de rede. Ela está correta?

6.3.5 Sugestões de tratamento

Se as configurações de rede do hospedeiro com máscara incorreta foram definidas manualmente, simplesmente corrija. Em máquinas Windows entre no Painel de Controle de Rede, escolha redes TCP/IP e pressione o botão Propriedades. Modifique a máscara de rede para o valor correto.

Em clientes Linux Slackware modifique o arquivo /etc/rc.d/rc.inet1. Ele contém as configurações da rede. Modifique a máscara de sub-rede para o valor correto. No Red Hat – e nos sistemas Linux baseados no sistema de inicialização System V – modifique o arquivo de configuração da interface envolvida no problema (que está com máscara de rede incorreta). No diretório /etc/sysconfig/network-scripts existe um arquivo de configuração para cada interface da máquina. Estes arquivos começam sempre com `ifcfg-`, seguidos do nome do dispositivo. Se você deseja modificar a máscara de rede da interface eth0, então edite o arquivo

ifcfg-eth0 e modifique o endereço configurado na linha que se inicia com `NETMASK`.

Após modificar a máscara para o valor correto reinicie o sistema operacional, seja ele qual for.

Se o escopo DHCP estava erroneamente configurado, será necessário modificá-lo e em seguida reiniciar o servidor DHCP. Em servidores Windows entre no Gerenciador DHCP como mostrado no teste confirmatório 2 e modifique a máscara de rede para o valor correto. Em seguida reinicie o servidor DHCP.

Em servidores DHCP Linux corrija a máscara de rede no arquivo /etc/dhcpd.conf (linha iniciada por `option subnet-mask`). Em seguida reinicie o servidor DHCP:

```
# /etc/rc.d/init.d/dhcp restart
```

Ou:

```
# kill –TERM <no. do processo dhcpd>[22]
# dhcpd
```

6.4 Cliente DNS mal configurado

6.4.1 Descrição

Para que a rede de uma máquina cliente funcione apropriadamente é necessário que seja configurado nela o endereço do servidor de nomes a ser utilizado quando necessário.

Quando o endereço do servidor de nomes não é especificado ou está incorreto, o serviço de nomes não funcionará para a máquina em questão. Como grande parte dos serviços de rede são acessados através de nomes de máquinas, o usuário da máquina com configuração de cliente DNS incorreta não conseguirá acessar vários serviços de rede.

6.4.2 Sintomas

Grande parte dos serviços de rede utilizados por usuários são acessados através dos nomes servidores. Quando o cliente DNS está apontando para um servidor de nomes errado ou não referencia servidor de nomes algum, a resolução de nomes não funcionará para a máquina em questão. Portanto, a partir desta máquina não será possível acessar serviços através dos nomes dos servidores, apenas de seus endereços IP.

---

[22] Este número pode ser obtido com o comando `# ps –ae | grep dhcpd`.

Nestes casos, a reclamação típica do usuário da máquina com cliente DNS mal configurado será de que a rede não está funcionando. Um usuário mais avançado pode utilizar endereços IP em vez de nomes e descobrir que o servidor responde quando se utiliza o seu IP, mas não responde quando o nome é utilizado.

6.4.3 Sinais

Procedimento
11.14

Serviços são acessados via endereço IP e não são acessados através do nome do servidor. A partir da máquina cliente com erro de configuração não é possível acessar certos serviços através do nome do servidor, mas o mesmo servidor é acessado através de seu endereço IP. Um cliente mais avançado, como citado na Seção **SINTOMAS**, pode observar este sinal.

6.4.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verifique o endereço IP do servidor de nomes configurado na máquina cliente;

TESTE 2

Se a máquina cliente for cliente DHCP verifique se o servidor DHCP está com escopo incorreto.

Teste confirmatório 1
O usuário da máquina certamente lhe informará o problema. Este teste é bastante simples: consiste apenas em verificar a configuração do cliente DNS na máquina do usuário reclamante. No procedimento ANALISANDO A CONFIGURAÇÃO DE REDE EM UM HOSPEDEIRO você encontrará dicas de como realizar este teste.

Teste confirmatório 2
Se a máquina com erro de configuração for cliente DHCP, é quase certo o erro de configuração do escopo DHCP. Este teste pode ser realizado conforme descrito no teste confirmatório 2 do problema **TABELA DE ROTAS DE HOSPEDEIROS INCORRETAS** No entanto, você estará procurando aqui não o endereço do roteador *default*, mas o endereço IP do servidor DNS.

6.4.5 Sugestões de tratamento

Corrija o erro de configuração do cliente DNS apropriadamente. No Windows veja as propriedades de configuração do protocolo TCP/IP e corrija o endereço IP do servidor DNS. No Linux corrija o erro reeditando o endereço IP do servidor DNS no arquivo /etc/resolv.conf.

Se o erro era no escopo do servidor DHCP, corrija-o e reinicie o servidor. Veja dicas de como corrigir o escopo do seu servidor DHCP nas sugestões de tratamento do problema **TABELA DE ROTAS DE HOSPEDEIROS INCORRETAS**. Mas lembre-se que neste momento você não procurará nem modificará o endereço do roteador default, mas do servidor de nomes.

6.5 Servidor DHCP mal configurado

6.5.1 Descrição

Leia mais sobre DHCP no apêndice 9

Um ou mais servidores DHCP mal configurados podem causar erros de configuração de endereçamento em hospedeiros em uma rede TCP/IP. Abaixo são listados alguns problemas que podem surgir quando se utiliza o serviço DHCP:

- O escopo está mal definido, podendo oferecer configurações erradas ou incompletas aos clientes DHCP;
    - Em um escopo DHCP são definidos parâmetros de configuração de rede que serão passados para os clientes DHCP. Configurações obrigatórias são: a faixa de endereços IPs que serão concedidos aos clientes, a máscara de sub-rede e o tempo de concessão. Outras opções comumente configuradas são os endereços IPs do roteador *default* e do(s) servidor(es) DNS. Este problema já foi indiretamente citado nos problemas de configuração de rede em hospedeiros apresentados anteriormente;
- Existe mais de um servidor DHCP na rede onde estão definidos escopos com faixas de endereços IPs sobrepostos, causando IPs duplicados na rede;
    - É comum que uma organização opte por possuir mais de um servidor DHCP. Assim, se um falhar, outro pode ainda estar funcionando. Infelizmente, não existe um protocolo padronizado que permita o espelhamento de um servidor DHCP. Cada servidor deverá ter sua própria configuração. Muito cuidado deve ser tomado para não configurar escopos sobrepostos em servidores diferentes;
    - O Windows 2000 oferece o serviço de *cluster* para alguns serviços, dentre eles, DHCP. Neste caso, muitos servidores DHCP coexistem em uma rede e se apresentam como se

fossem apenas um, oferecendo um serviço de mais alta disponibilidade;

- Alguns servidores e clientes DHCP mais novos (os do Windows ME e 2000, por exemplo) se protegem contra endereço IP duplicado, não permitindo que isto ocorra. Desta forma, mesmo que os servidores DHCP estejam com escopos sobrepostos, não serão observados IPs duplicados na rede. Isto torna a detecção e localização dos escopos sobrepostos mais difícil. Por outro lado, as versões mais antigas do DHCP não têm esta proteção, possibilitando a ocorrência deste problema mais facilmente devido a um descuido durante a configuração dos servidores DHCP. Portanto, um cuidado redobrado deve ser tomado quando múltiplos servidores DHCP coexistem em ambientes mais antigos;

- O valor do tempo de concessão de um endereço pode estar inadequado;
  - O tempo de concessão é o tempo durante o qual o cliente DHCP pode utilizar o endereço que lhe foi fornecido pelo servidor. De tempos em tempos (sempre que se passa a metade do tempo de concessão), o cliente tenta renovar seu contrato, o que pode ou não ser aceito pelo servidor. Não existe um tempo de concessão ideal, devendo este se adequar ao comportamento da rede. Mais detalhes em **SUGESTÕES DE TRATAMENTO**.
- O número de máquinas ativas na rede é maior que o número de endereços IP disponíveis no servidor DHCP;
  - A conseqüência deste fato é que um hospedeiro irá solicitar suas configurações de rede e elas não serão enviadas pelo servidor, uma vez que não existem mais endereços disponíveis;
  - Um tempo de concessão pequeno reduz um pouco os efeitos deste problema, mas tem a desvantagem de diminuir o poder de rastreamento. Com um tempo de concessão de 1 hora, por exemplo, é mais difícil – e se o log do servidor DHCP não estiver habilitado é praticamente impossível – descobrir com firmeza qual era a máquina que possuía determinado IP há dois dias.
- O serviço DHCP, por algum motivo, não foi inicializado, ou foi interrompido;
  - Os clientes não obterão resposta à sua requisição DHCP e ficarão sem configuração de rede;
- Se um agente de repasse estiver em uso, certificar-se de que não existe filtro IP barrando a passagem do tráfego DHCP;

- Os endereços IPs dos servidores DHCP estão incorretos no agente de repasse;

6.5.2 Sintomas

Quando o servidor DHCP está com o escopo mal configurado todos os hospedeiros configurados através do servidor serão afetados. Esse problema leva a configurações de rede erradas ou incompletas em hospedeiros. Por exemplo, quando o escopo DHCP do servidor está configurado com o roteador *default* incorreto, os clientes DHCP serão configurados com um endereço de roteador *default* errado, e apresentarão determinados sintomas. Na Seção **SINTOMAS** dos problemas **TABELA DE ROTAS DE HOSPEDEIROS INCORRETAS**, **ENDEREÇO IP DE HOSPEDEIRO INCORRETO**, **HOSPEDEIRO COM MÁSCARA DE REDE INCORRETA** e **CLIENTE DNS MAL CONFIGURADO** são apresentados os sintomas para cada um dos erros de configuração possíveis de ocorrer.

Se o tempo de concessão estiver muito pequeno, não existirão sintomas, apenas alguns sinais. Por outro lado, em uma rede muito dinâmica, onde máquinas entram e saem da rede em pequenos intervalos de tempo, um tempo de concessão muito grande pode levar à falta de endereços IP. A conseqüência percebida pelos usuários será falta de conectividade durante um certo tempo para as máquinas que não conseguirem obter suas configurações de rede de imediato.

Suponha um tempo de concessão de 20 horas e um escopo contendo 32 IPs. Nas primeiras 5 horas de funcionamento do servidor DHCP 20 máquinas são ligadas e 20 IPs concedidos a elas pelo servidor. Duas destas vinte máquinas foram logo desligadas. Passadas as primeiras 5 horas, 14 novas máquinas foram inseridas na rede. O servidor, no entanto, pensa que apenas 12 IPs estão disponíveis. Durante as próximas 15 horas 2 máquinas ficarão sem conectividade. Passadas as 15 horas, o tempo de concessão dos primeiros IPs concedidos (para as máquinas que foram desligadas) expirará. Só então as 2 máquinas obterão suas configurações de rede. Este exemplo é ilustrado na Figura 6-1.

Os demais problemas citados na seção anterior levam à falta de conectividade, uma vez que os hospedeiros não obterão suas configurações de rede.

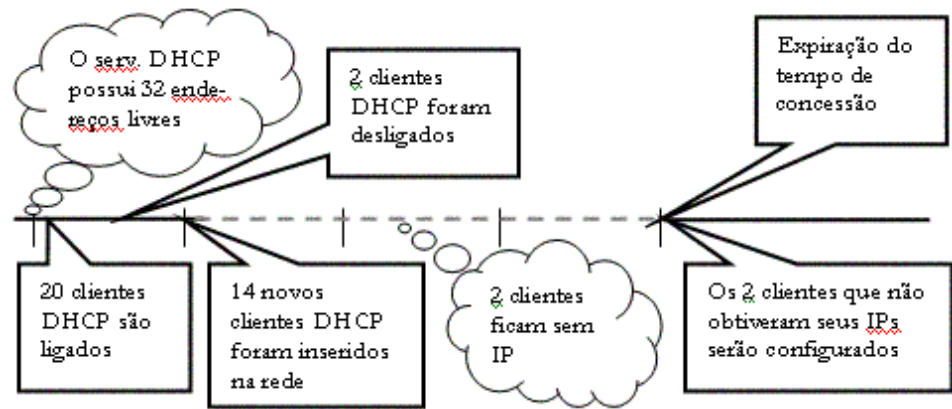



Figura 6-1: Exemplo do funcionamento do servidor DHCP

6.5.3 Sinais

Quando o escopo está incorretamente configurado, os sinais dependem do tipo de erro existente. Os sinais percebidos são os mesmos apresentados na Seção SINAIS dos problemas **TABELA DE ROTAS DE HOSPEDEIROS INCORRETAS**, **ENDEREÇO IP DE HOSPEDEIRO INCORRETO**, **HOSPEDEIRO COM MÁSCARA DE REDE INCORRETA** e **CLIENTE DNS MAL CONFIGURADO**. Em resumo, os sinais apresentados serão:

Procedimento **11.2**

- Quando a máscara de rede estiver configurada com um valor menor que o valor real trafegarão na rede requisições ARP, sem a resposta correspondente.

Procedimento **11.13**

- Além disso, poderão ser encontradas nas tabelas de rotas de hospedeiros, rotas específicas para outros hospedeiros. Isto também ocorrerá quando a tabela de rotas do hospedeiro estiver incompleta.

Procedimento **11.8**

- Quando a máscara de rede estiver configurada com um valor maior que o valor correto ou a tabela de rotas estiver incompleta, várias mensagens ICMP REDIRECT serão encontradas na rede;

Procedimento **11.1**

- Quando existirem IPs duplicados na rede serão encontradas pelo menos duas respostas à mesma requisição ARP;

Procedimento **11.14**

- Quando o endereço do servidor de nomes de domínio estiver incorreto ou não estiver configurado serviços serão acessados via endereço IP e não serão acessados através do nome do servidor.

Procedimento **11.6**

Comumente, o cliente DHCP renova o aluguel de seu IP mantendo o mesmo endereço IP. Mesmo que o tempo de concessão de um endereço IP já tiver expirado, o servidor DHCP, em princípio não oferecerá este IP a um outro cliente. Mas, quando a quantidade de endereços IP é pequena em relação à

quantidade de máquinas na rede, o servidor DHCP pode ser obrigado a reutilizar um endereço IP cujo tempo de concessão expirou. Antes de oferecer este endereço o servidor certifica-se de que o cliente que o possui não o está mais utilizando. Quando o cliente DHCP que originalmente possuía o endereço IP requisitá-lo novamente, o servidor responderá ao cliente com uma mensagem DHCPNAK, indicando que não pode mais oferecer este endereço ao cliente. Portanto, em redes onde o número de máquinas é maior que o número de endereços IP a serem alocados, encontraremos constantemente mensagens DHCPNAK.

Procedimento **11.5**

Quando todos os endereços IPs do servidor já tiverem sido distribuídos entre os clientes e um novo cliente requisitar suas configurações de rede, o servidor DHCP informará a falta de endereços IPs ao administrador da rede através de mensagens escritas nos logs do servidor DHCP. Este é um sinal diferencial que confirma a falta de endereços IPs para serem distribuídos pelo servidor DHCP aos seus clientes.

Procedimento **11.7**

Se existir um filtro IP barrando o tráfego DHCP (UDP 67 para servidor e UDP 68 para clientes), nenhuma requisição externa de clientes DHCP será encontrada na rede;

Procedimento **11.4**

Se o servidor DHCP não estiver ativado ou os endereços dos servidores DHCP estiverem incorretamente configurados em um agente de repasse DHCP, trafegarão na rede mensagens DHCP REQUEST sem resposta de qualquer servidor DHCP. Após requisições DHCP espera-se que o(s) servidor(es) DHCP retorne(m) mensagens do tipo DHCPOFFER.

6.5.4 Testes confirmatórios

Como apresentado na Seção **DESCRIÇÃO**, são várias as causas do mal funcionamento da alocação dinâmica de IPs utilizando servidores DHCP. Muitas vezes, a causa do mau funcionamento pode ser descoberta através dos sintomas/sinais observados. Se você, por exemplo, encontrou nos *logs* do servidor que não existem mais IPs disponíveis, um problema já foi confirmado.

Antes de cada teste descrito a seguir é apresentado um breve resumo de como a rede se comporta se estiver com o problema que será testado. Infelizmente não existe uma MIB DHCP (ainda!) e todos os testes são dependentes de um analisador de protocolos ou do tipo de servidor DHCP utilizado.

RESUMO DOS TESTES

TESTE 1 — Verifique se o servidor DHCP está em execução;

TESTE 2 — Verifique a configuração do escopo definido no servidor DHCP;

TESTE 3 — Verifique a configuração de rede enviada para os clientes pelo servidor DHCP (com um analisador de protocolos);

TESTE 4 — Verifique as configurações do agente de repasse DHCP;

TESTE 5

Se existir um filtro IP, certifique-se de que ele permite a passagem do tráfego DHCP;

Se os clientes DHCP não estiverem conseguindo se comunicar com o servidor DHCP, todos eles ficarão sem configurações de rede. Certifique-se, primeiramente, que o servidor DHCP está em execução:

Teste confirmatório 1

No Windows verifique se o servidor DHCP está em execução e certifique-se de que ele está sendo iniciado sempre automaticamente. No Windows 2000 escolha Iniciar > Programas > Ferramentas Administrativas > Serviços. Clique com o botão direito do mouse sobre o Servidor DHCP e escolha o item Propriedades. Verifique se o serviço está habilitado e sendo automaticamente iniciado. No Windows NT o Gerenciados de Serviços pode ser obtido através do Painel de Controle.

No Linux, certifique-se de que o `dhcpd` está em execução com o comando:

```
# ps.-ae | grep dhcpd
```

Certifique-se também de que ele está sendo iniciado automaticamente. Em um Linux Slackware os comandos a seguir lhe informarão se o serviço DHCP está sendo iniciado automaticamente e em que script de inicialização.

```
# grep dhcp /etc/rc.d/rc*
```

Se nenhum script de inicialização está iniciando o serviço DHCP você confirmou o problema. Caso você encontre um arquivo que inicie o serviço DHCP certifique-se de que este arquivo está realmente sendo executado durante a inicialização da máquina.

Em máquinas Linux baseadas no *System V* – como Red Hat, por exemplo – a verificação é um pouco diferente. Verifique se em algum diretório rc existe um *link* iniciado com a letra “S” que aponta para o arquivo /etc/rc.d/init.d/dhcpd.

```
# grep dhcp /etc/rc.d/*/S*
```

Se as configurações de rede de todos os clientes DHCP estão apresentando problemas, é provável que o escopo configurado no servidor DHCP esteja incorreto ou incompleto. Realize o teste confirmatório a seguir.

Teste confirmatório 2

Verifique a configuração do escopo no servidor DHCP. Comumente, são definidos em um escopo os seguintes itens: a faixa de endereços IPs a serem alocados aos clientes, o endereço IP do roteador *default*, a máscara de sub-rede e o endereço IP do servidor de nomes do domínio[23]. Eventualmente, podem ser destacados endereços IPs dentro da faixa configurada que não podem ser alocados a clientes, isto é, estão reservados para máquinas com IP fixo. Analise as configurações do servidor DHCP e certifique-se de que ela está correta.

Para acessar o gerenciador do servidor DHCP no Windows NT clique em Iniciar > Programas > Ferramentas Administrativas > Gerenciador DHCP. Clique com o mouse sobre o escopo desejado e no menu Escopo, selecione o item Propriedades. Surgirá uma janela informando a faixa de endereços IPs configurada, a máscara de rede, os endereços reservados e o tempo de concessão escolhido. Para visualizar outras opções escolha no menu Opções DHCP o item Escopo e verifique as configurações das opções escolhidas. Para visualizar as configurações é necessário que o servidor esteja em execução.

No Windows 2000 clique em Iniciar > Programas > Ferramentas Administrativas > DHCP. Navegue no escopo em questão (interface semelhante ao Windows Explorer) e verá os valores de cada item no painel à direita.

No Linux verifique as configurações do servidor DHCP no arquivo /etc/dhcpd.conf.

Se existir a suspeita de IPs duplicados na rede realize os testes confirmatórios problema **ENDEREÇO IP DE HOSPEDEIRO INCORRETO**.

Um teste interessante é também verificar que valores de configuração de rede os clientes DHCP estão recebendo do servidor. Este teste é apresentado no teste confirmatório 3 abaixo.

Teste confirmatório 3

Com um analisador de protocolos capture os pacotes DHCP trocados entre servidor e os clientes. Obtenha dicas de como

[23] Outras configurações mais específicas de ambientes Windows podem também ser repassadas. Por exemplo, endereço IP do servidor WINS.

conectar o analisador de protocolos e criar o filtro DHCP no UTILIZANDO UM ANALISADOR DE PROTOCOLOS.

Quando um cliente solicita seus parâmetros de rede ao servidor, ele enviará um quadro de difusão do tipo DHCPDISCOVER com endereço fonte igual a 0.0.0.0. O servidor DHCP responderá com um pacote DHCPOFFER, que já informa um possível IP para o cliente. O cliente responde com um DHCPREQUEST, e o servidor então lhe envia um DHCPREPLY, que informa o valor de todas as opções configuradas no escopo em uso (IP do roteador *default*, do servidor de nomes, por exemplo).

Analise os pacotes DHCPREPLY enviados pelo servidor, pois neles estão contidas todas as configurações de rede passadas para o cliente DHCP. Você pode encontrar com este teste configurações que passaram despercebidas no teste confirmatório 1.

Teste confirmatório 4

Se um agente de repasse DHCP estiver em uso, certifique-se de que ele está corretamente configurado. Isto é, se o IP do servidor DHCP está correto. Em um roteador Cisco série 7500, por exemplo, use o comando a seguir para ver quais os servidores DHCP conhecidos pelo roteador:

```
roteador# show dhcp server
```

Teste confirmatório 5

Se existir um filtro IP entre os clientes e o servidor DHCP, tenha certeza de que é permitida a entrada e saída de tráfego UDP nas portas 67 e 68.

6.5.5 Sugestões de tratamento

Uma vez encontrado o problema de configuração do servidor DHCP ou do agente de repasse, refaça a configuração solucionando o problema. Em geral, a solução será mais simples que a localização exata do problema com o serviço DHCP.

Se você descobriu que o serviço DHCP não está sendo iniciado automaticamente a correção também é clara: configure o serviço para que ele seja iniciado automaticamente. No Windows isto pode ser feito com o auxílio

do Gerenciador de Serviços do Windows (Iniciar > Programas > Ferramentas Administrativas > Serviços no Windows 2000 ou ícone Serviços no Painel de Controle do Windows NT). Configure o serviço corretamente, de forma que ele fique em execução e seja iniciado automaticamente. Para certificar-se de que suas correções estão corretas, reinicialize a máquina onde o servidor está instalado e em seguida veja se o serviço DHCP está em execução. No Linux Slackware o serviço DHCP deve ser ativado no arquivo /etc/rc/rc.inet2.

Se o servidor DHCP informou através de seus *logs* que não tinha mais IPs para oferecer aos clientes ou for observada a presença constante de mensagens DHCPNAK na rede, obtenha/configure mais endereços IP para seu escopo. Diminuir o tempo de concessão também pode ajudar. Talvez seja necessário passar a utilizar endereços privativos. Desta forma, não será necessário solicitar a quem competir (seu provedor, por exemplo) uma nova faixa de endereços IP.

Veja um exemplo: em curtos intervalos de tempo máquinas saem e entram em sua rede. O tempo de concessão está em 5 horas. Com este tempo de concessão, por algumas horas o servidor DHCP pode pensar que todos os endereços estão alocados, embora algumas máquinas nem participem mais da rede. Quando novas máquinas forem inseridas na rede, não haverá mais (do ponto de vista do servidor) IPs para estas máquinas, e elas ficarão sem configuração de rede. Se o tempo de concessão for menor, o servidor DHCP perceberá mais rapidamente que determinadas máquinas não estão mais na rede e a falta de endereços IPs ocorrerá em menor número.

Como exemplificado acima, o valor configurado para o tempo de concessão é importante para o melhor funcionamento da alocação dinâmica de IPs em uma rede. Infelizmente, não existe um número mágico que represente o melhor tempo de concessão. Cada rede possui suas características próprias, e o tempo de concessão deve ser configurado com base nessas características.

Se o número de máquinas em uma rede é maior que o número de IPs disponíveis, um tempo de aluguel menor (1 hora, por exemplo) é mais interessante. Nos casos em que o número de máquinas é menor que o número de IPs disponível, o tempo de aluguel pode ser maior, chegando até a meses. Faça uma análise levando em consideração a quantidade de máquinas clientes em sua rede e a quantidade de endereços IPs disponíveis. Veja outros exemplos e uma análise mais detalhada sobre o tempo de concessão de um servidor DHCP em [DHCP_FAQ].

Uma outra questão que pode ser levada em consideração é a facilidade de rastreamento diante de incidentes de segurança. Uma das máquinas da sua rede pode ter sido invadida. O invasor instalou nela um código malicioso que é executado para invadir servidores de outra organização. O administrador da organização que sofreu a tentativa de invasão informará o IP da máquina da qual partiu o ataque e a data e hora da tentativa. De posse destas informações você tentará descobrir que máquina está invadida. Quando o número de endereços IPs disponíveis é maior que o número de máquinas, é comum que cada cliente DHCP continue alocando sempre o mesmo IP. No entanto, é possível que um outro IP seja alocado ao cliente. Se o tempo de concessão for maior – um mês, por exemplo – você sabe que durante, pelo menos um mês

uma máquina está sempre com o mesmo IP. Se o tempo de concessão for menor – uma hora, por exemplo – será mais difícil identificar que máquina estava com determinado IP em um certo dia.

6.6 Rotas estáticas mal configuradas

6.6.1 Descrição

Leia mais sobre rotea-mento no apêndice 8

Em algumas organizações as tabelas de rotas – ou parte delas – são construídas manualmente, pelo gerente da rede. A construção estática das tabelas de rotas dos roteadores tem suas vantagens e desvantagens. Nela, nenhuma largura de banda precisa ser consumida para a troca de informações de roteamento entre roteadores. Além disso, o processador dos roteadores não é empregado para a construção das tabelas de rotas, ficando livre para outras atividades. Por outro lado, o gerente que configura as rotas estáticas precisa conhecer bastante a topologia da rede e atualizar o roteamento sempre que uma nova rede for adicionada.

Neste problema são apresentados erros que comumente ocorrem quando rotas estão sendo estaticamente configuradas nos roteadores da rede. Alguns problemas subseqüentes analisarão alguns erros quando o protocolo RIP está sendo utilizado para a construção dinâmica das tabelas de rotas dos roteadores.

Rotas estáticas mal configuradas levam a tabelas de rotas incorretas, que podem causar laços lógicos entre roteadores e falta de rotas. A Figura 6-2 mostra um exemplo de laço lógico entre roteadores. O pessoal do Departamento de Recursos Humanos não consegue comunicação com o Departamento de Finanças nem de Vendas. Os dados originados no Departamento de Finanças ou Vendas com destino ao Departamento de Marketing circularão entre roteador1 e roteador2 até que o TTL se esgote.

Além de laços entre roteadores, a má configuração das rotas pode levar a tabelas de rotas incompletas. Uma tabela de rotas está incompleta quando um roteador recebe um datagrama, mas não sabe para onde enviá-lo por não existir em sua tabela de rotas uma entrada que o informe para onde enviar o datagrama.

Considere, por exemplo, que o comando

```
# route add –net 192.168.10.0 –netmask 255.255.255.0 –gw
192.168.13.1
```

devesse ser executado em um roteador para adicionar uma certa rota[24].

No entanto, por erro de digitação, o comando executado foi

```
# route add –net 192.168.19.0 –netmask 255.255.255.0 –gw
192.168.13.1.
```

[24] Este comando informa que datagramas com destino à rede 192.168.10.0/255.255.255.0 devem ser entregues ao roteador 192.168.13.1.

Alguns dos possíveis efeitos colaterais deste descuido são:

- erroneamente, os datagramas com destino à rede 192.168.19.0/24 serão enviados para o roteador 192.168.13.1. Eles deveriam, por exemplo, seguir a rota *default*;
- o roteador não saberá para onde enviar os datagramas destinados a máquinas da rede 192.168.10.0/24 ou, se existir rota *default*, ela será utilizada;
- este comando pode sobrescrever a rota correta para a rede 192.168.19.0/24.

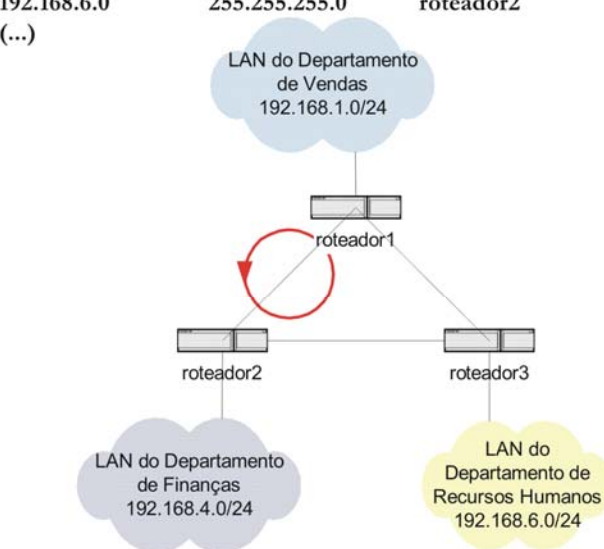



Figura 6-2: exemplo de laço entre roteadores

Por fim, um cuidado especial deve ser tomado ao configurar buracos negros (*black holes*). Suponha que sua organização possui uma classe B de endereços. Você quebrou esta faixa em várias sub-redes. No entanto, nem todas as sub-redes possíveis estão sendo utilizadas. Então você configura o seu roteador para jogar fora os datagramas com destino a sub-redes que não estão em uso – isto é um buraco negro. Configurações incompletas de buracos negros podem ser a causa de problemas. Ao configurá-los em um ambiente estático (que não utiliza protocolos de construção dinâmica de tabela de rotas), é obrigatória a inserção das rotas para as sub-redes em uso. Caso contrário os datagramas destinados a elas cairão erroneamente no buraco negro. Um exemplo de erro deste tipo é apresentado no teste confirmatório 3 da Seção **TESTES CONFIRMATÓRIOS**.

6.6.2 Sintomas

Em geral, todas as situações de erro de configuração de rotas levam a destinos inalcançáveis. Os usuários reclamarão de falta de conectividade para uma ou mais redes.

6.6.3 Sinais

Procedimento **11.9**

Quando laços lógicos existirem, muitas mensagens ICMP Time Exceeded (ICMP tipo 11, código 0) trafegarão na rede. Cada vez que um datagrama passa por um roteador, o valor do campo TTL é decrementado de 1. Se um roteador está processando um datagrama e percebe que o TTL é zero, ele deve descartar o datagrama. Após o descarte, ele deve notificar a máquina que originou o datagrama com uma mensagem ICMP de tempo excedido. Portanto, quando existe um laço lógico entre roteadores, os datagramas circularão no laço até que o TTL chegue a zero, sendo descartados e mensagens *ICMP Time Exceeded* são enviadas às origens dos datagramas. Mensagens desse tipo idealmente não são encontradas na rede.

Procedimento **11.10**

Quando faltam entradas na tabela de rotas de um roteador, Destination Unreachable Messages (ICMP tipo 3, código 0) são encontradas na rede. Se um roteador receber um datagrama e não souber para onde enviá-lo, ele descartará o datagrama e transmitirá uma mensagem *ICMP Destination Unreachable* para a máquina origem do datagrama. O ideal é que mensagens deste tipo não existam na rede.

Procedimento **11.11**

Idealmente, a variável `ipOutNoRoutes` (da MIB-2) não é constantemente incrementada. Ela tem seu valor aumentado sempre que uma das seguintes situações ocorre:

- quando datagramas são descartados porque não existem rotas que possam ser seguidas por ele;
- quando o roteador *default* para onde o datagrama deveria ser enviado não está operacional.

Portanto, o crescimento rápido do valor da variável ipOutNoRoutes pode indicar erros na tabela de rotas.

6.6.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Localize o erro. Quais os roteadores que provavelmente estão mal configurados?

TESTE 2

Analise as tabelas de rotas dos roteadores envolvidos;

TESTE 3

Verifique a configuração de buracos negros;

Teste confirmatório 1

Para localizar o problema, a melhor ferramenta a ser utilizada é o `traceroute` (`tracert` no Windows). Esta ferramenta mostra todo o percurso seguido por datagramas IP desde a origem até o destino. Com esta ferramenta pode-se detectar rapidamente laços e analisar o caminho seguido pelos datagramas IP. Quando o erro se trata de falta de rotas, o `traceroute` permite a identificação do roteador além do qual a comunicação não mais existe.

Ao suspeitar de erro de roteamento, conecte-se em uma máquina e execute o `traceroute` direcionado a outra máquina. Analise a saída. A rota seguida é a esperada? Existem laços? O datagrama chega no destino? Os exemplos a seguir ilustram dois tipos comuns de erros: o primeiro mostra um laço entre roteadores e o segundo um destino inalcançável.

Considere novamente o exemplo da Figura 6-2. O gerente de vendas da empresa liga para o gerente da rede e reclama que não consegue usar a aplicação de cadastro de vendedores. Após alguns segundos de conversa o gerente de vendas diz que a rede está funcionando normalmente, só não consegue usar esta aplicação. O gerente de rede deduz que não há comunicação entre o Departamento de Vendas e o Departamento de Recursos Humanos, onde está a aplicação de cadastro de vendedores. O gerente de redes então se conecta em uma máquina do Departamento de Vendas e direciona um `traceroute` para o servidor da aplicação em questão, obtendo a seguinte saída:

```
# traceroute –n 192.168.6.10

1   0.132 ms   0.211 ms   0.217 ms   192.168.1.254

2   0.231 ms   0.165 ms   0.153 ms   192.168.2.254

3   0.214 ms   0.189 ms   0.344 ms   192.168.1.254

4   0.254 ms   0.213 ms   0.222 ms   192.168.2.254

5   0.235 ms   0.198 ms   0.210 ms   192.168.1.254

6   0.301 ms   0.255 ms   0.278 ms   192.168.2.254

...
```

Como se vê acima, um laço entre os roteadores 192.168.1.254 e 192.168.2.254 foi identificado

Em uma outra situação de erro (não mais considerando o exemplo da Figura 6-2), a saída poderia ser:

```
# traceroute –n 192.168.6.10
```

```
1   0.132 ms   0.211 ms   0.217 ms   192.168.13.1
2   0.231 ms   0.165 ms   0.153 ms   192.168.15.3
3   0.214 ms   0.189 ms   0.344 ms   192.168.17.3
4   !H    !H    !H
5   !H    !H    !H
...
```

Neste exemplo, o datagrama não vai além do roteador 192.168.17.3, sendo possível que uma ou mais rotas estejam faltando neste roteador, ou que rotas incorretas tenham sido configuradas nos roteadores anteriores.

O caminho percorrido pelos datagramas é o esperado? Se for, o problema é na tabela de rotas dos roteadores envolvidos no laço, ou do roteador que não sabe para onde enviar o datagrama. Se o caminho seguido pelos datagramas não foi o esperado, a tabela de rotas do roteador a partir do qual o caminho é desviado deve estar com problemas.

Teste confirmatório 2

Uma vez localizado o erro de roteamento, a próxima atividade a ser realizada é analisar as tabelas de rotas dos roteadores que ficaram sob suspeita. Este já é na realidade o primeiro passo para a correção do problema. No exemplo apresentado anteriormente, seria interessante examinar as tabelas de rotas dos roteadores 192.168.2.254 e 192.168.2.253 no caso em que o laço foi detectado e do roteador 192.168.17.3 no outro caso. Esta análise pode ser feita através de um terminal de gerência ou com o auxílio de uma estação de gerência SNMP. O **PROCEDIMENTO 11.3** mostra como analisar a tabela de rotas de um roteador.

Analise as tabelas de rotas dos roteadores sob suspeita para confirmar o erro de roteamento. Para realizar esta tarefa a equipe de gerência deve saber qual seria a tabela de rotas correta. Em outras palavras, a equipe deve entender perfeitamente a topologia da rede e qual o roteamento desejado. Caso contrário, novos erros podem ser introduzidos.

Teste confirmatório 3

Se buracos negros tiverem sido configurados, certifique-se de que todas as sub-redes em uso têm uma rota configurada. Se você esquecer de inserir as rotas para as sub-redes que estão em uso, os datagramas enviados para elas serão perdidos no buraco negro. O exemplo a seguir ilustra a situação.

Considere uma organização que possui uma classe B de endereços IP. Internamente, esta classe foi dividida em diversas sub-redes classe C: a sub-rede do *backbone* e sub-redes dos diversos departamentos. No entanto, apenas os 10 primeiros endereços estão sendo utilizados. O gerente da rede cria então, no roteador de entrada do *backbone* um buraco negro para evitar que datagramas com IP destino inexistente circulem na rede. A Figura 6-3 ilustra a rede mencionada neste exemplo.

Em um roteador Cisco 7507, por exemplo, basta criar a interface lógica null0 e executar o comando

```
roteador# ip route 155.190.0.0 255.255.0.0 null0
```

A partir de então, todos os datagramas destinados a uma sub-rede de 155.190.0.0/16 para a qual não exista uma rota específica serão jogados no buraco negro. Portanto, antes de adicionar a rota para o buraco negro, rotas para sub-redes em uso devem ser adicionadas. Por descuido, o gerente da rede citada no exemplo da Figura 6-3 adicionou as rotas para 9 redes, mas esqueceu da rede 155.190.3.0/24. Resultado: a comunicação entre máquinas da rede 155.190.3.0/24 e outras máquinas não será possível sempre que roteador-ext for um nó intermediário.

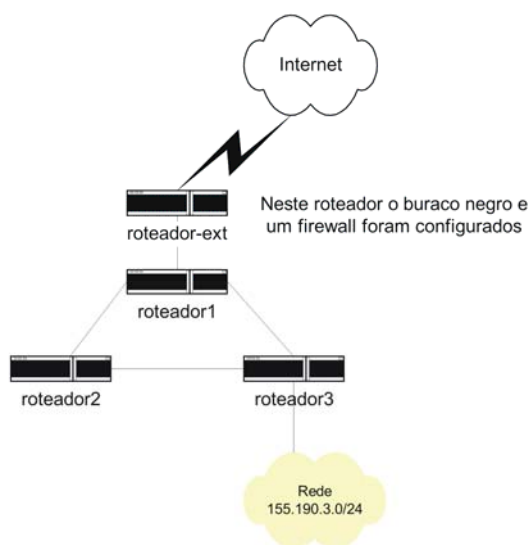



Figura 6-3: mapa da rede mencionada no exemplo de buraco negro

6.6.5 Sugestões de tratamento

Após a detecção e localização do erro, corrija a tabela de rotas incorreta. Essa correção deve ser realizada com cuidado, e mudanças só devem ser realizadas quando a equipe de gerência estiver certa de que a modificação é correta. O ideal é que esta correção seja feita por duas pessoas juntas, para que a possibilidade de introdução de novos erros seja a mínima possível.

Se você tem que atualizar tabelas de rotas mais de uma vez por mês, ou se em sua rede existirem enlaces de redundância, o ideal é que você comece a usar um protocolo de construção dinâmica de tabela de rotas tal como RIP ou OSPF.

6.7 Equipamento inserido em VLAN incorreta

6.7.1 Descrição

Leia mais sobre VLANs no apêndice 12

Em um ambiente de VLANs configuradas por portas, os seguintes cuidados devem ser tomados:

- ao transferir um membro da VLAN de uma porta para outra do comutador, certifique-se de que ele continuará pertencendo à VLAN apropriada;
- quando for inserir um novo membro na VLAN, verifique se ele foi inserido na VLAN correta, isto é, foi conectado em uma porta que participa da VLAN apropriada.

Da mesma forma, quando as VLANs são configuradas por endereço MAC, os seguintes cuidados devem ser tomados:

- ao mudar o endereço MAC de um membro da VLAN, o novo endereço deve ser cadastrado na VLAN e o antigo desconsiderado;
- quando novas máquinas são inseridas na rede, o endereço MAC deve ser cadastrado na VLAN apropriada;

Considere a configuração das VLANs da Figura 6-4. Nesta figura, duas VLANs são configuradas: as primeiras 4 portas de comutador1 (da esquerda para a direita) fazem parte da VLAN 1 e as demais portas da VLAN 2. Certo dia, os serviços oferecidos por servidor1 não estavam disponíveis. Maria, que era nova na equipe de gerência, antes de tentar isolar o problema corretamente, resolveu simplesmente conectar o servidor a outra porta do comutador. Servidor1 foi, então, conectado à porta 4 do comutador, que pertence à VLAN 1. A topologia da rede passou a ser a apresentada na Figura 6-5. Com esta mudança, servidor1 ficou incomunicável, pois está conectado à VLAN incorreta. O roteamento para a rede 192.168.2.0/24 e, conseqüentemente, para servidor1, sempre levará à VLAN 2, impossibilitando qualquer comunicação dos clientes com o servidor, que agora está participando fisicamente da VLAN 1.

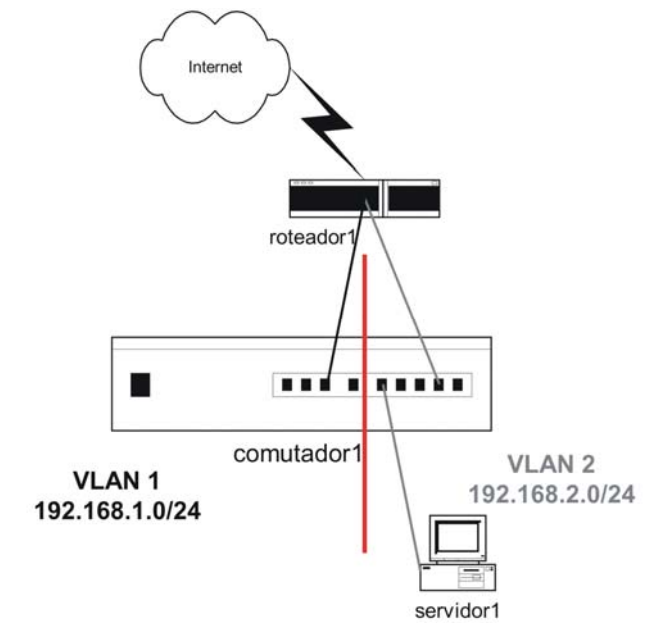



Figura 6-4: VLANs configuradas por porta

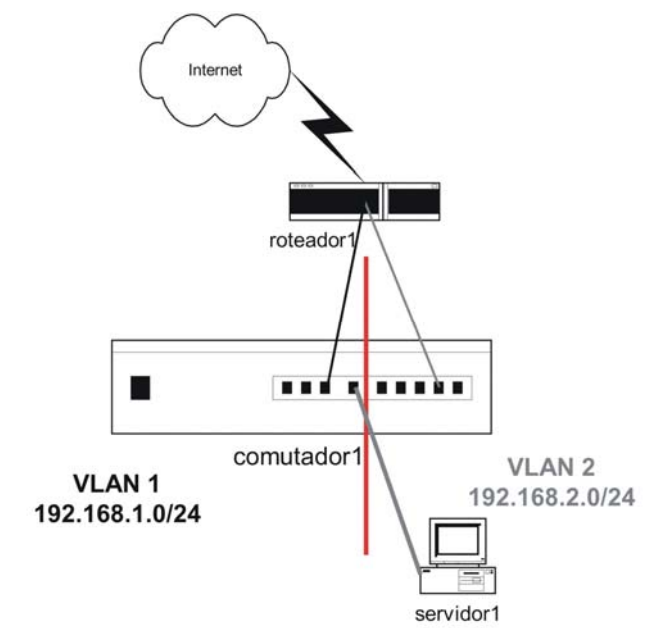



Figura 6-5: Nova disposição das máquinas.

Em um ambiente de VLANs configuradas por porta ou por endereço MAC, sempre que uma nova máquina for inserida na rede, o gerente deve certificar-se de que a máquina será conectada na VLAN correta. Caso contrário, a máquina será inserida em uma VLAN *default* e não se comunicará com outras máquinas da rede apropriadamente.

É possível também que este problema ocorra quando as VLANs por porta ou por MAC estiverem sendo configuradas – erro de configuração. Existe ainda uma última possibilidade: um usuário mesmo troca, sem comunicar à gerência, a posição do cabo no comutador ou sua placa de rede. Este é o pior caso, pois a modificação foge do controle do time de gerência.

6.7.2 Sintomas

O sintoma deste problema é sempre falta de conectividade ou indisponibilidade de alguns serviços, mas as reclamações vindas dos usuários podem ser diferentes, dependendo do tipo de equipamento transferido de uma VLAN para a outra e de como este equipamento está configurado:

- Sendo uma máquina cliente, o usuário desta máquina poderá sentir:
  - falta de conectividade
  - a falta de conectividade ocorrerá em duas situações: 1) quando o endereço IP da máquina é configurado estaticamente, e 2) quando o endereço IP da máquina é dinâmico, mas a partir da nova VLAN nenhum servidor DHCP é alcançável;
  - não conseguir mais utilizar alguns serviços
  - o endereço IP da máquina é configurado dinamicamente. Na nova VLAN um servidor DHCP concedeu à máquina cliente novas configurações de rede. A máquina continuará com conectividade, mas não poderá utilizar os serviços que só eram permitidos para a antiga configuração de rede. Por exemplo, a maioria dos servidores POP só aceitam clientes que possuem endereços dentro de uma certa faixa de endereços IP;
- Sendo um repetidor ou outro comutador onde estão ligadas máquinas clientes:
  - Idem anterior. No entanto a reclamação partirá de vários usuários e não apenas de um. Portanto, vários usuários irão reclamar de falta de conectividade ou de não conseguirem mais utilizar alguns serviços;.
- Sendo um servidor:
  - os usuários do servidor reclamarão que não conseguem mais utilizar os serviços oferecidos por ele. Em geral, servidores possuem endereços configurados estaticamente, portanto, o servidor não será mais alcançável ao mudar de VLAN;
- Sendo um roteador:
  - se o roteador em questão é o responsável pelo roteamento entre as VLANs, a VLAN da qual o roteador não mais participa passa a ficar incomunicável. Os membros desta VLAN só irão se comunicar entre si;
  - se o roteador em questão dá acesso a outras redes, os usuários destas redes reclamarão de falta de conectividade com uma ou mais redes.

6.7.3 Sinais

Os sinais estarão espalhados em várias VLANs e até nas máquinas afetadas pela modificação. Na VLAN original[25], serão percebidos os seguintes sinais:

Procedimento **11.2**

Requisições ARP trafegam sem resposta. Com a mudança, a máquina passa a fazer parte fisicamente de outra VLAN, onde os quadros de difusão de sua VLAN original não chegam. Por isto, sempre que alguém desejar falar com esta máquina, requisições ARP serão enviadas (seja pelo roteador ou por membros da VLAN original) e nenhuma resposta será dada. Este sinal será mais visível quando a máquina em questão for um servidor e máquinas clientes tentarem utilizar seus serviços.

Procedimento **11.10**

O roteador conectado à VLAN onde a máquina deveria estar inserida não mais conseguirá falar com ela. Serão enviadas para todos os que desejam falar a máquina em questão mensagens ICMP Host Unreachable. Quando um roteador tenta fazer uma entrega direta de um datagrama ao destinatário e percebe que este está inalcançável, ele envia uma mensagem ICMP *Destination Unreachable* (tipo 3, código 1) à origem do datagrama informando o fato. Esta mensagem diz que o equipamento final ao qual o datagrama foi endereçado não é alcançável no momento.

Se a máquina envolvida na modificação tem suas configurações de rede obtidas estaticamente, na VLAN onde a máquina foi inserida erroneamente o sinal será o seguinte:

Procedimento **11.12**

Tráfego de difusão cujo endereço origem não faz parte do conjunto de endereços configurados nas máquinas da VLAN. Muitos serviços de rede dependem do envio de quadros de difusão. Quando uma máquina está inserida na VLAN incorreta, encontraremos nesta VLAN quadros de difusão enviados por uma máquina que não deveria fazer parte desta Esta máquina tem prefixo de rede diferente das demais máquinas da VLAN.

Se a máquina que foi conectada em outra VLAN tiver suas configurações rede obtidas através de um servidor DHCP, outros sinais podem ser observados na máquina em questão e na VLAN onde ela foi inserida:

Procedimento **11.13**

Se existir um servidor DHCP ou um agente de repasse DHCP na VLAN onde a máquina foi erroneamente inserida, a máquina continuará obtendo dinamicamente suas configurações de rede[26]. No entanto, as configurações recebidas são de outra sub-rede, isto é, um endereço IP de outra faixa de endereços, um outro roteador *default*, e possivelmente outro servidor de nomes e outra máscara de rede. A máquina, que deveria fazer parte de uma determinada rede, vai apresentar configurações de outra rede.

---

[25] Considere VLAN original a VLAN da qual a máquina deveria estar participando.

[26] Para tornar o serviço DHCP mais seguro, pode-se amarrar endereços lógicos a endereços físicos. Neste caso, a configuração de rede também não será obtida, pois o MAC da nova máquina inserida não está configurado no servidor DHCP.

Procedimento 11.13

Se na VLAN onde a máquina foi erroneamente inserida não existir um servidor DHCP ou um agente de repasse DHCP, a máquina não obterá qualquer configuração de rede, apresentará o endereço 0.0.0.0 como seu endereço de rede, endereço de servidor de nomes e máscara de rede.

6.7.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Você tem um ambiente de VLANs configuradas por portas ou por endereço MAC?

Caso a VLAN seja configurada por porta:

TESTE 2

Verifique a disposição das máquinas nas portas do comutador. Alguma modificação foi realizada?

Se a VLAN for configurada por endereço MAC:

TESTE 3

Verifique se o endereço MAC de algum equipamento membro da VLAN foi modificado (uma máquina inteira ou uma placa de rede foi substituída);

Teste confirmatório 1

Muito provavelmente, os usuários irão reclamar. Se você observou os sinais e sintomas descritos nas seções anteriores, e se os usuários que se queixaram estão em um ambiente de VLANs configuradas por porta ou por endereço MAC, este problema pode estar ocorrendo. Você ou a equipe de gerência realizou alguma troca que pode ter causado o problema? Se alterações foram feitas, realize o teste confirmatório 2 (para VLANs definidas por porta) ou o teste confirmatório 3 (para VLANs configuradas por endereço MAC).

Se você tem um ambiente de VLANs configuradas por MAC ou por porta, mas você ou a equipe de gerência não realizou modificações que possam ter causado o problema, ainda assim, este problema pode estar ocorrendo. Não é raro que usuários mais audaciosos realizem trocas que causem este problema.

Por algum motivo, o usuário não está conseguindo ler seus e-mails. Ele acha que a rede não está funcionando. O que ele faz? Levanta-se de sua cadeira, vai até o equipamento de interconexão onde sua máquina está ligada e vê que existem algumas portas vazias. Ele simplesmente transfere o cabo de sua máquina para uma dessas portas vazias. Quando vai testar a modificação vê que a rede continua sem funcionar e então resolve ligar para o gerente da rede para fazer sua reclamação. Por esta razão, é importante

conversar calmamente com os usuários e coletar deles o máximo de informações. Se for possível que usuários realizem esta troca, isto é, se os usuários têm acesso aos comutadores, realize o teste confirmatório 2.

Se você tem VLANs configuradas por endereço MAC e é permitido aos usuários a substituição de suas placas de rede por outras, realize o teste confirmatório 3.

Teste confirmatório 2

Com o auxílio da documentação da rede, verifique se os cabos de rede estão conectados nas portas corretas do comutador. Em uma rede bem documentada, todos os cabos são identificados e no próprio comutador onde as VLANs estiverem configuradas existirá alguma etiqueta informando quais portas pertencem a quais VLANs.

Se sua rede não estiver bem documentada, verifique a configuração das VLANs no próprio comutador. Na maioria dos comutadores Cisco, por exemplo, você pode verificar a configurações das VLANs com o comando:

```
Console> show vlan
```

Se os cabos também não estiverem identificados você vai ter que descobrir de onde vem cada cabo manualmente para se certificar de que estão conectados nas devidas portas. Anote quais os LEDs do comutador estão acesos. Desconecte o cabo de uma máquina que está conectada ao comutador e verifique qual o LED que apagou quando o cabo foi desconectado. Realize este teste para cada um dos equipamentos conectados ao comutador e aproveite para identificá-los e atualizar sua documentação.

Teste confirmatório 3

Considerando VLANs definidas por MAC, se você ou sua equipe realizou alguma das seguintes alterações, o problema foi confirmado.

- substituição de membro da VLAN por outro. Por exemplo, o usuário foi presenteado com uma máquina nova;
- substituição de placa de rede. A placa antiga apresentou defeito, por exemplo, e você teve que substituí-la. Ao final da

substituição, a rede não funciona, e você está pensando que é a placa nova;

Se você desconhece a ocorrência de alguma destas alterações, certifique-se de que os usuários não as realizaram. É menos comum que usuários troquem suas placas de rede, pois eles geralmente não têm conhecimento em redes suficiente para tal ato. Além disso, é uma boa prática de gerência que esta tarefa só seja permitida a membros da equipe de gerência com a devida permissão. Mas, quando se trata de usuário, tudo é possível. É mais comum que usuários adquiram novas máquinas e não consigam mais utilizar a rede. Enfim, converse com os usuários afetados em busca de mudanças que possam ter causado o problema. Se máquinas ou placas de rede foram substituídas o problema foi confirmado.

6.7.5 Sugestões de tratamento

Se o problema ocorreu devido a um descuido da própria equipe de gerência durante a configuração das VLANs, simplesmente corrija o erro.

Se o problema foi causado pela equipe de gerência é provável que a sua rede não esteja bem documentada. Por exemplo, no exemplo apresentado na Seção **DESCRIÇÃO**, se existisse uma etiqueta no comutador informando quais VLANs estão configuradas e que portas pertencem a cada uma delas, talvez a troca não tivesse sido realizada. Ou, se no comutador ou na máquina cliente fosse informado quais máquinas participam de cada VLAN por MAC, a substituição de uma máquina sem o recadastramento da mesma na VLAN apropriada ocorreria com menos freqüência.

Para evitar inserir novos problemas ao tentar solucionar um problema, como ocorreu no exemplo apresentado, organize a documentação da sua rede. Mais informações sobre documentação de rede podem ser encontradas no Apêndice 5 e em [PERF&FAULT CISCO].

Se foi um usuário o causador do problema e se você percebe que os usuários estão constantemente realizando modificações sem o seu conhecimento, comece a pensar em uma forma de proibir o acesso de usuários a equipamentos de interconexão, lacre as máquinas, desabilite administrativamente as portas de comutadores vagas e proíba que certas configurações (como as configurações de rede) possam ser realizadas por eles. Comece a pensar também em oferecer um serviço de gerência mais eficaz, pois essa **pode** ser uma dica de que os usuários não confiam no desempenho e agilidade de sua equipe de gerência e acham que podem resolver o problema mais rapidamente que vocês.

6.8 VLANs não estão configuradas

6.8.1 Descrição

Ver mais sobre VLANs no apêndice 12

Considere a seguinte situação:

Maria, suporte técnico de redes, chega na sala da gerência e, imediatamente, o telefone toca: reclamações… Uma das sub-redes da empresa não está funcionando segundo um certo usuário. Ela observa através da ferramenta de gerência que realmente a reclamação procede: roteadores, enlaces e comutadores estão todos com alarme crítico. Enquanto ela observava a ferramenta de gerência outros 4 telefonemas de reclamações são recebidos. Maria, ainda inexperiente, quer logo resolver o problema. Ela descobre que a causa do problema é um determinado comutador, pois seus LEDs estão indicando a existência de algo anormal, segundo a documentação do comutador. Maria, prontamente, reinicializa o comutador, com esperanças de que ele voltará ao normal. No entanto, os LEDs continuam indicando problemas. Enquanto isso, mais telefonemas…

Maria, já desesperada, resolve substituir o comutador defeituoso por outro que está funcionando corretamente. E assim o faz. Ela esqueceu, no entanto, de verificar na documentação da rede se no comutador substituído existiam VLANs configuradas. E, para seu azar, existiam. Após substituir o comutador Maria achou que tinha resolvido o problema, mas alguns usuários continuavam reclamando.

Quando o chefe de Maria chegou, ele explicou o que havia acontecido: Maria não considerou a possibilidade de existência de VLANs no comutador e o substituiu. No entanto, o comutador defeituoso possuía três VLANs configuradas por porta – as primeiras 8 portas faziam parte da VLAN 1, as 8 portas seguintes da VLAN 2 e as demais da VLAN 3. Quando Maria substituiu o comutador por outro sem configuração apropriada de VLANs, ela trouxe várias máquinas, de sub-redes diferentes, para uma mesma VLAN, isto é, para um mesmo domínio de difusão. Com isso os quadros de difusão de uma sub-rede passam a ser recebidos também pelas máquinas da outra sub-rede. Serviços que se utilizam de quadros de difusão, como DHCP, por exemplo, começaram a apresentar um comportamento estranho.

No caso apresentado acima, cada uma das VLANs tem seu próprio servidor DHCP. Em todas as VLANs, algumas máquinas têm configuração de rede fixa e outras obtêm suas configurações através de DHCP. O problema pode ocorrer em máquinas que têm a rede configurada dinamicamente. Pode ocorrer de uma máquina de uma determinada sub-rede requisitar sua configuração de rede (via endereço de difusão) e receber primeiro a resposta de um servidor DHCP de outra sub-rede. Neste caso, a máquina até continuará se comunicando na rede, no entanto não conseguirá acessar alguns serviços que só são permitidos às máquinas que possuem certos endereços IP.

Na realidade, a troca de um comutador por outro sem a preocupação em trazer toda a configuração do antigo comutador para o novo é problemática também em outros sentidos. Por exemplo, o novo comutador pode não estar com o

Protocolo Árvore de Cobertura habilitado – o que pode causar problemas. O endereço IP do novo comutador pode não estar configurado, ou ser diferente (provavelmente será) do endereço do antigo comutador. A aplicação de gerência, por exemplo vai acusar que o comutador está não operacional. Em resumo, o único equipamento que podermos substituir sem realizar qualquer verificação de configuração é um repetidor não gerenciável. Até nos repetidores gerenciáveis precisamos configurar pelo menos o IP correto para que a estação de gerência consiga falar com ele.

6.8.2 Sintomas

VLANs limitam domínios de difusão. Quando todas as máquinas de várias VLANs diferentes são inseridas erroneamente numa única VLAN, dependendo da quantidade de máquinas que passam a fazer parte do mesmo domínio de colisões e dos serviços oferecidos e utilizados por elas, a grande quantidade de tráfego de difusão pode tornar a rede lenta.

No entanto, o problema mais grave ocorre quando serviços que dependem de difusão são utilizados. A seguir mostramos um exemplo do que pode ocorrer com o serviço DHCP.

É possível que dois ou mais servidores DHCP passem a coexistir no mesmo domínio de difusão. Se não existir a associação entre endereço MAC e endereço IP configurados em cada servidor DHCP, quando um cliente DHCP solicitar suas configurações de rede duas situações podem ocorrer:

1. Por coincidência o servidor DHCP correto responde primeiro. A máquina cliente adquire as configurações de rede corretas e tudo funciona bem. Neste caso, nenhuma reclamação será feita;

2. Outro servidor DHCP responde à requisição do cliente DHCP e oferece ao cliente certas configurações de rede. Neste caso, é possível que haja:

    2.1. não funcionamento de certos serviços → muitos serviços que o cliente requisitará só são permitidos a clientes que possuem endereço IP dentro de uma certa faixa. Então, os usuários reclamarão que não conseguem acessar certos serviços. Por exemplo, os usuários não conseguirão ler e receber mensagens, pois os servidores SMTP e POP geralmente não aceitam conexões de qualquer cliente, apenas de clientes que possuem certos endereços IP[27];

    2.2. falta de conectividade → as configurações oferecidas pelo servidor DHCP são incompletas. O cliente DHCP esperava receber, dentre outros parâmetros o roteador *default*, mas o servidor

[27] Se existe apenas um servidor de cada serviço para toda a organização, ou pelo menos para todos os usuários das VLANs que foram unidas, então este sintoma não existirá;

que respondeu não estava configurado para oferecer este parâmetro;

Estas são algumas situações levantadas. Agora imagine a quantidade de serviços que dependem de quadros de difusão. O *logon* Windows é um outro serviço que pode começar a apresentar problemas. Enfim, diversas reclamações podem surgir, dependendo de quais serviços são utilizados.

6.8.3 Sinais

Procedimento **10.9**

Quantidade excessiva tráfego de quadros de difusão. A quantidade de quadros de difusão que trafegam em um domínio de difusão depende da quantidade de máquinas no domínio de difusão e dos serviços oferecidos. É aceitável que uma máquina envie aproximadamente 1 quadro de difusão a cada 10 segundos. Sendo assim, em um domínio de difusão com N máquinas, será normal que trafeguem na rede, aproximadamente, N/10 quadros de difusão por segundo. Em um domínio com 1000 máquinas, por exemplo, o tráfego médio de difusão será de aproximadamente 100 quadros de difusão por segundo. Os processadores de equipamentos mais modernos conseguem processar alguns milhares de quadros de difusão por segundo sem comprometer o desempenho da rede. Mas, em geral, estabelecemos limiares bem menores para a quantidade de quadros de difusão por segundo encontrados em uma rede.

Alguns comutadores possuem a funcionalidade de suprimir o tráfego de difusão. Eles podem ser configurados para aceitar até uma certa quantidade de quadros de difusão por segundo (limiar), e descartar os demais quadros, e neste caso, deve-se observar se o limiar estabelecido não está sendo constantemente alcançado.

Procedimento **10.6**

Utilização alta de CPU. Uma quantidade excessiva de quadros de difusão trafegando na rede pode saturar os processadores de equipamentos de interconexão e hospedeiros. Com o aumento vertiginoso da quantidade de quadros de difusão, a taxa de utilização da CPU dos equipamentos de interconexão e hospedeiros irá crescer bastante em relação ao normal, e poderá chegar a alcançar 99/100%. Em geral, taxas médias de utilização de CPU superiores a 75% já devem ser investigadas.

Procedimento **10.10**

Saturação da largura de banda. A quantidade excessiva de quadros de difusão aumenta a utilização dos enlaces que participam do domínio de difusão. Será observado um aumento da utilização dos enlaces em relação ao tráfego normal da rede. Com um tráfego de difusão de 1000 quadros por segundo, considerando quadros de difusão de 64 bytes, o tráfego de difusão é de 1000 x 64 x 8 = 512 Kbps.

Procedimento **11.12**

Máquinas que fazem parte de uma determinada sub-rede passam a receber quadros de difusão de máquinas de outra sub-rede. Isto ocorrerá quando existirem máquinas que têm configurações de rede estáticas. Por exemplo, sem a configuração correta de VLANs, a máquina 128.128.10.1 da sub-rede 128.128.10.0/24, que pertencia a uma determinada VLAN, passa a receber quadros destinados ao endereço de difusão 128.128.11.255, que é de outra sub-rede e originalmente pertencia a outra VLAN.

Procedimento
11.13

Quando as configurações de rede das máquinas são obtidas dinamicamente, é possível encontrar máquinas que deveriam fazer parte de uma sub-rede com configurações de outra sub-rede. Isto ocorrerá quando mais de um servidor DHCP passar a existir no mesmo domínio de colisões e o servidor "errado" responder à requisição do cliente.

6.8.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1 — Houve a substituição de algum comutador?

TESTE 2 — O novo comutador está com as VLANs corretamente configuradas?

Teste confirmatório 1

Este problema só[28] ocorrerá quando alguém – mais provavelmente um membro da equipe de gerência – substituir um comutador por outro sem considerar a possibilidade da existência de VLANs. É muito improvável que um usuário faça isto, portanto, este é um problema de rápida e fácil localização. Os sintomas do problema serão percebidos pelos usuários afetados, que reclamarão. A equipe de gerência deve, então se perguntar, se alguma substituição de comutador foi feita que possa ter causado o problema. Caso a resposta a esta questão seja positiva, realize o teste confirmatório 2.

Teste confirmatório 2

Se no comutador antigo estavam configuradas VLANs e no novo não, ou outras VLANs estavam configuradas, o problema foi confirmado. Verifique no novo comutador se as VLANs estão adequadamente configuradas.

Para visualizar as configurações de VLAN em comutadores Cisco Catalyst série 6000 use o comando:

```
console> (enable) show vlan
```

Comutadores mais antigos, Cisco Catalyst 1900, por exemplo, as VLANs configuradas podem ser vistas escolhendo-se, no menu

[28] É possível também que o comutador apresente problemas e por isso as VLANs sejam desconfiguradas, mas este já é um problema de nível físico (**EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSO**) que acarretou a desconfiguração das VLANs.

principal, a opção `Virtual Lan`. Em comutadores IBM 8271-712 escolha a opção `Switch Management`. No nível de gerência de VLANs selecione a opção `Setup`. Uma tabela informando de que VLAN cada porta participa é apresentada.

Analise as configurações de VLAN do comutador. Elas estão corretas? Caso a resposta seja negativa o problema foi confirmado.

6.8.5 Sugestões de tratamento

A solução para este problema é configurar as VLANs. Esta seção nem deveria existir para este problema, não fossem as seguintes importantes dicas:

Documente sua rede. Por exemplo, nos comutadores onde VLANs estão configuradas, anexe etiquetas que informem quais são as VLANs e suas configurações. Assim, quando alguém tiver que substituir um comutador por outro vai lembrar das VLANs e configurá-las no novo comutador.

Uma excelente prática de gerência de configuração, já mencionada no problema **EQUIPAMENTO DE INTERCONEXÃO DEFEITUOSO**, é organizar a linha base de configuração da rede (veja mais informações na página 60). Se a linha base de configuração existisse, ao substituir um comutador por outro ela seria usada, e nenhum erro ocorreria.

6.9 Comutadores não conseguem trocar informações sobre VLANs entre si

6.9.1 Descrição

Aprenda mais sobre VLANs no apêndice 12

VLANs limitam domínios de difusão. Na teoria, uma VLAN pode atravessar vários comutadores. Por exemplo, uma VLAN por porta pode envolver portas de vários comutadores diferentes. Quando uma VLAN atravessa muitos comutadores, é necessário que eles saibam como trocar entre si informações sobre as VLANs. Quando um comutador recebe um quadro de difusão, ele precisa saber a que VLAN o quadro pertence para então enviar este quadro a todos os membros da VLAN. Além disso, é necessário que o comutador saiba que existem membros da VLAN em outros comutadores, e envie para estes comutadores os quadros de difusão recebidos dos membros da VLAN.

Quando a VLAN é definida por endereço IP, a identificação da VLAN já é carregada implicitamente no quadro, através do próprio endereço IP da estação que o enviou. No entanto, quando se trata de VLANs definidas por porta ou endereço MAC a identificação da VLAN deve ser realizada explicitamente [VLAN-REPORT]. Isto é, de alguma forma um comutador precisa identificar a que VLAN um quadro pertence.

Considere as VLANs 1 e 2 definidas na Figura 6-6.

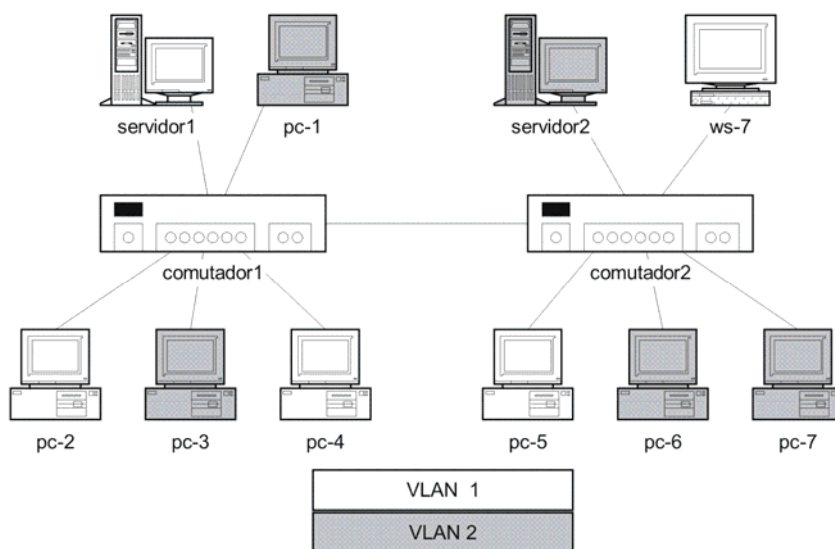



Figura 6-6: VLANs que atravessam comutadores.

Comutador1 e comutador2 precisam se comunicar para trocar informações sobre as VLANs definidas neles. Cada um precisa saber que parte dos membros de cada VLAN definida está conectada diretamente e parte está conectada no comutador vizinho. Além disso, quando comutador1 vai enviar um quadro para comutador2, é preciso que ele identifique a que VLAN o quadro pertence.

Quando quadros de difusão são enviados em um ambiente de VLANs, apenas os membros da mesma VLAN de quem originou o quadro de difusão devem recebê-lo. É aí que reside o problema: se comutador1 e comutador2 não estiverem conversando a mesma língua, eles não entenderão que parte da VLAN 1 está conectada em um comutador e parte em outro. O mesmo ocorre com a VLAN 2. Quando pc-1 enviar um quadro de difusão, apenas pc-3, que também está diretamente conectado a comutador1, receberá o quadro.

Comutadores podem trocar entre si informações sobre VLANs de três formas distintas: mantendo uma tabela via sinalização, TDM e etiquetamento de quadros, sendo a última a técnica mais utilizada [VLAN-REPORT]. Nesta abordagem, a identificação da VLAN é adicionada nos quadros que irão atravessar enlaces entre comutadores. Estes enlaces que ligam comutadores (ou comutadores e roteadores) passam a se chamar troncos e carregam o tráfego de várias VLANs distintas entre comutadores e roteadores. No exemplo da Figura 6-6 o enlace que liga comutador1 e comutador2 é um tronco pelo qual trafegam dados da VLAN 1 e da VLAN 2.

A variedade de tipos de VLANs e de formas de comunicação entre comutadores para a troca de informações sobre VLANs levaram cada fabricante de comutadores a desenvolver sua própria solução para VLANs. A conseqüência é que a solução de VLANs de um fabricante quase sempre não é compatível com a de outro fabricante. Isto obriga os consumidores que desejam configurar VLANs que atravessam múltiplos comutadores a comprar produtos de um único fabricante.

Para solucionar este problema de interoperabilidade a IEEE propôs o padrão 802.1Q, que segue a abordagem do etiquetamento de quadros. A maioria dos novos comutadores já adota este padrão. Este problema é mais comum quando comutadores mais antigos são usados (ou se a configuração do tronco não estiver correta).

Em comutadores Cisco mais novos, por exemplo, dois tipos de codificação estão disponíveis: o ILS (Inter-Switch Link), que é proprietário da Cisco, e o 802.1Q, que é o padrão.

Quando VLANs que atravessam vários comutadores são definidas e os comutadores envolvidos não sabem trocar entre si informações sobre as VLANs, todos os serviços que dependem de difusão ficam comprometidos. Abaixo seguem exemplos do que ocorre com alguns serviços que se utilizam do envio de quadros de difusão.

O serviço ARP, de mapeamento de endereços lógicos em endereços físicos, depende do envio de quadros de difusão. Devido à falta de comunicação entre os comutadores, a troca de informações entre membros de uma mesma VLAN que estão conectados em comutadores diferentes não será possível – exceto se o mapeamento "endereço lógico" → "endereço físico" for estaticamente configurado nos membros das VLANs. Mais adiante será dado um exemplo deste caso.

Um outro serviço importante que pode ser prejudicado é o DHCP. Considere que servidor2 é o servidor DHCP dos membros da VLAN 2. Como conseqüência da falta de interoperabilidade entre comutador1 e comutador2 no que diz respeito a VLANs, pc-1, que é um cliente DHCP não poderá obter suas configurações de rede.

6.9.2 Sintomas

O sintoma percebido pelos usuários depende de que serviços baseados em quadros de difusão estão sendo utilizados pelos membros das VLANs. No exemplo da Figura 6-6, o usuário de pc-1 reclamaria de falta de conectividade ou, em linguagem de usuário, que a rede não está funcionando, já que ele não consegue obter suas configurações de rede.

Um outro sintoma pode ser o não funcionamento de alguns serviços mesmo que eles não sejam baseados no envio de quadros de difusão. Este sintoma ocorrerá na seguinte situação: 1) servidor e cliente pertencem à mesma VLAN, mas estão conectados em comutadores distintos; 2) os comutadores não estão conseguindo trocar informações sobre VLANs entre si; 3) baseado em suas configurações de rede o cliente sabe que deve fazer uma entrega direta ao servidor e 4) o cliente sabe apenas o endereço lógico do servidor. O protocolo ARP deverá ser utilizado pelo cliente, que deseja descobrir o endereço físico do servidor. Veja o exemplo a seguir:

Considere que servidor2 também é servidor POP. Para se conectar a servidor2, pc-3 precisa, primeiro saber qual o endereço físico do servidor. Para tal, o

protocolo ARP será utilizado. No entanto, apenas pc-1 receberá o quadro de difusão ARP. Sem resposta, a conexão entre pc-3 e servidor2 não será possível.

Considere a mesma situação envolvendo, no entanto, duas máquinas clientes. Neste caso, o sintoma será falta de conectividade entre máquinas clientes.

Se você tem uma rede Microsoft e não estiver utilizando servidor WINS[29], alguns clientes reclamarão de não conseguir efetuar o *logon* na rede. Uma outra reclamação será de não conseguir navegar em todas as máquinas da rede[30]. Isto se deve ao fato de que nas redes Microsoft, tanto o serviço de *logon* quanto o de navegação em outras máquinas da rede são baseados no envio de quadros de difusão. Por exemplo, para encontrar o controlador de domínio primário (servidor que autenticará os usuários na rede) os clientes enviam um quadro de difusão na rede. Se o controlador de domínio primário estiver em outro comutador, o quadro de difusão enviado pelo cliente não chegará no controlador, e o cliente não poderá ser autenticado. Provavelmente o cliente será informado de que o controlador de domínio primário não pôde ser encontrado, ou não existe.

Considerando, por exemplo, que servidor1 é controlador de domínio primário, o usuário de pc-5 não conseguirá sequer efetuar *logon* na rede e o usuário de pc-2 e pc04 não enxergarão pc-5 como máquina de seu ambiente de rede.

Os serviços mais comuns foram escolhidos para serem dados como exemplo nesta seção. No entanto, outros sinais podem surgir, dependendo dos serviços oferecidos em sua rede e de como ela está configurada.

6.9.3 Sinais

Assim como os sintomas, os sinais que podem ser identificados dependem de que serviços dependentes do envio de quadros de difusão estão configurados nas VLANs. Os sinais abaixo consideram os serviços ARP, DHCP.

Procedimento **11.2**

Como mostrado em exemplo anterior, os quadros de difusão que carregam requisições ARP só serão enviados para os membros da VLAN que estão conectados no mesmo comutador. Desta forma, serão encontradas na rede requisições ARP sem resposta.

Procedimento **11.4**

Requisições DHCP sem resposta do servidor DHCP. Este caso também foi ilustrado com um exemplo anteriormente. Se o servidor e o cliente DHCP participam da mesma VLAN mas estão em comutadores distintos, se os comutadores não estiverem trocando informações sobre VLANs adequadamente, o servidor não receberá a requisição ARP do cliente, que ficará sem resposta.

[29] Quando você configura um servidor WINS em seu domínio e configura as estações de trabalho para utilizá-lo (via DHCP ou manualmente), o *logon* e a navegação em outras máquinas da rede passam a ser um processo que não envolve envio de quadros de difusão.

[30] Ao abrir uma janela do Windows Explorer e clicando no ícone "Toda a rede", um usuário pode navegar em outras máquinas da rede Microsoft.

Procedimento

11.13

Clientes DHCP sem as configurações de rede. Este sinal, é na realidade uma conseqüência do sinal anterior. Como o cliente DHCP não conseguiu falar com o servidor DHCP, o cliente DHCP ficará sem suas configurações de rede e apresentará o endereço 0.0.0.0 seu como endereço IP e máscara de rede.

6.9.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Você configurou VLANs que atravessam mais de um comutador?

TESTE 2

Os comutadores envolvidos pertencem a fabricantes distintos?

TESTE 3

Qual o protocolo utilizado para troca de informações sobre VLANs entre os comutadores?

Teste confirmatório 1

Este problema só ocorrerá quando VLANs são estendidas por mais de um comutador. Os comutadores mais antigos não suportam ainda os novos padrões propostos e ainda trocam informações sobre VLANs utilizando soluções proprietárias. Se você acabou de configurar VLANs que abrangem mais de um comutador e está observando os sintomas e sinais descritos anteriormente, grandes chances existem de você estar utilizado comutadores que não conseguem trocar informações sobre VLANs entre si.

Teste confirmatório 2

Verifique se os comutadores envolvidos são do mesmo fabricante. Caso não sejam, as chances deste problema estar ocorrendo são maiores.

Teste confirmatório 3

Verifique o tipo de codificação utilizada nos troncos. Em comutadores Cisco mais novos execute o comando:

```
Console> (enable) show trunk
```

Ele lhe mostrará, dentre outras informações, quais os troncos configurados e que tipo de codificação estão utilizando. Verifique o tipo de codificação dos troncos em todos os comutadores e roteadores que participam das VLANs. Se os tipos de codificação não forem compatíveis o problema foi confirmado.

Considere novamente o exemplo Figura 6-6. Você teria que se conectar em comutador1 e verificar a configuração dos troncos existentes. Em seguida fazer os mesmo com comutador2.

6.9.5 Sugestões de tratamento

Infelizmente, as sugestões de tratamento para este problema são bastante caras:

- voltar atrás, isto é, não estender VLANs por mais de um comutador;
- comprar novos comutadores que suportem o padrão 802.1Q;
- utilizar apenas os comutadores de um mesmo fabricante.

Em comutadores Cisco Catalyst série 6000 o seguinte comando deverá ser utilizado na configuração de um tronco 802.1Q em uma porta:

- `set trunk mod/port [on | desirable | auto | nonegotiate] dot1q`

O comando a seguir configura um tronco 802.1Q na porta 1 do módulo 1 de um comutador Cisco [CISCO-VLAN-TRUNKS]:

```
Console> (enable) set trunk 1/1 desirable dot1q
```

Se você ainda não comprou os comutadores, mas já está planejando configurar VLANs que atravessam múltiplos comutadores, leve em conta este problema ao escolher os comutadores que serão adquiridos. Compre comutadores que já suportem o padrão ou compre todos os comutadores de um mesmo fabricante.

6.10 Ambiente RIP-1 com VLSM e/ou redes não contíguas

6.10.1 Descrição

Leia mais sobre RIP no capítulo X

O protocolo RIP-1 foi projetado para ser usado com endereços que pertençam às classes A (máscara 255.0.0.0), B (máscara 255.255.0.0) ou C (máscara 255.255.255.0) definidas. Por esta razão, as mensagens RIP-1 não trazem consigo informações de máscaras de sub-redes. No entanto, com o tempo, sub-redes e super-redes começaram a ser utilizadas para um melhor aproveitamento dos endereços IP e para diminuir a as tabelas de rotas dos roteadores. Isto leva a existência de redes com máscaras que não pertencem a nenhuma das classes, ou ainda a redes que, por exemplo, teoricamente deveriam ter máscara de uma certa

classe, mas têm outra máscara (configuração de sub-redes). Como as mensagens RIP-1 não trazem consigo informações de máscaras de rede, um roteador RIP-1 só está autorizado a enviar o anúncio de uma rota se ele tiver certeza de que os roteadores que receberão o anúncio saberão aplicar a máscara de rede correta à rota anunciada [RFC 2453].

Para tal, ao compor suas mensagens de atualizações de roteamento, um roteador RIP-1 realiza alguns testes para certificar-se de que os recipientes da mensagem saberão "inferir" a máscara de rede de cada rota corretamente. Em resumo[31], os roteadores que participam de sub-redes semelhantes (com mesmo prefixo classe A, B ou C e mesma máscara de sub-rede) à sub-rede a ser anunciada, receberão o anúncio para a sub-rede. No entanto, para os roteadores que não participam de uma sub-rede semelhante, as rotas para as sub-redes serão sumariadas em uma única rota para a rede classe A, B ou C ou nada será anunciado. Ao receber mensagens de atualização RIP-1, muitos roteadores aplicam a mesma máscara de rede configurada na interface que recebeu a atualização de roteamento [RFC 2453]. Os exemplos a seguir esclarecerão melhor o problema.

Leia mais sobre endereçamento no apêndice 8

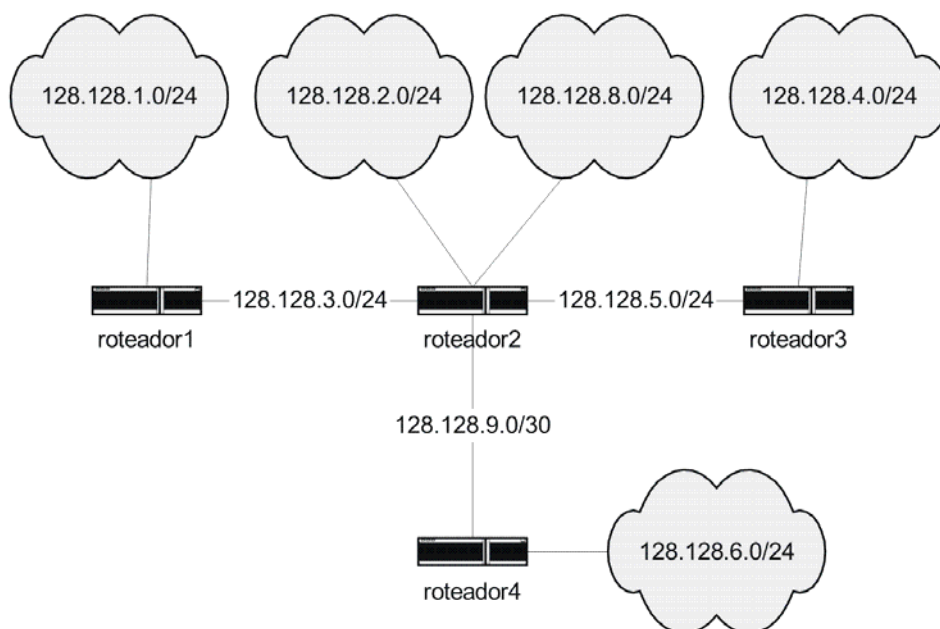



Figura 6-7: Rede com VLSM (Variable Length Subnet Mask).

Na Figura 6-7, roteador1, roteador2 e roteador3 participam, cada um, de uma ou mais sub-redes semelhantes da rede 128.128.0.0/16. As máscaras de todas as sub-redes são iguais, com valor 255.255.255.0. Desta forma, roteador2 poderá enviar para roteador1 e roteador3 anúncios de rotas das sub-redes 128.128.2.0 e 128.128.8.0. Roteador1 e roteador3 aplicarão à rota recebida de roteador2 a mesma máscara das interfaces que receberam a atualização de roteamento. No entanto, para roteador4, roteador2 nada anunciará sobre suas sub-redes, uma vez que este não está certo de que roteador4 será capaz de inferir corretamente

[31] Em [CISCO-RIP-BEHAVIOR, CISCO-RIP-VLSM E CISCO-RIP-DISCONTIGUOUS] é apresentada uma visão mais detalhada do comportamento de um roteador RIP ao enviar e receber mensagens de atualizações de rotas.

as máscaras de suas sub-redes. Quando roteador4 receber um datagrama destinado à rede 128.128.1.0/24, por exemplo, não saberá para onde enviar, exceto se existir uma rota *default* configurada e esta rota coincidir com a rota que deveria ser utilizada.

Como conseqüência de seu modo de operação, o protocolo RIP-1 também não é apropriado para ser utilizado em redes não contíguas. Se a rede que ligasse roteador2 e roteador4 não tivesse o prefixo 128.128 – fosse, por exemplo, 200.128.1.0/24 – estaria configurada a não contigüidade. Duas sub-redes de mesmo prefixo *classful* passam a ser separadas por uma outra rede, com um prefixo diferente. Neste caso, roteador2 anunciaria para roteador4 a rota para a rede 128.128.0.0.

Em resumo, só faz sentido que um roteador propague uma rota com máscara M e prefixo de rede P por uma interface que também tenha máscara M e prefixo de rede P. Se a máscara for outra e o prefixo for P nada será anunciado e se a máscara for M, mas o prefixo for outro a rota será sumariada para a rota classe A, B ou C.

6.10.2 Sintomas

É difícil prever o comportamento do roteamento em um ambiente RIP-1 com VLSM e/ou redes não contíguas. Em geral, os usuários reclamarão de falta de conectividade para uma ou mais redes. No exemplo da Figura 6-7, os usuários das LANs 128.128.1.0/24 e 128.128.6.0/24 reclamariam de falta de conectividade entre si.

6.10.3 Sinais

Procedimento

11.10

Quando VLSMs são configuradas em um ambiente RIP-1, as tabelas de rotas ficarão incompletas. Neste caso, para alguns destinos, o roteador não saberá qual o próximo roteador para o qual o datagrama deve ser enviado. Na Figura 6-7, por exemplo, roteador4 não saberá rotear pacotes destinados à rede 128.128.2.0/24, pois devido à existência de máscaras de sub-redes variáveis, roteador2 não anunciou esta rede para roteador4. Se existir rota default, ela será usada sempre que a rota específica para um certo destino não for encontrada. Se nenhuma rota default estiver configurada, o roteador não saberá para onde enviar o datagrama, sendo este descartado. Após descartar o datagrama, o roteador transmitirá uma mensagem ICMP Destination Unreachable para a máquina origem do datagrama. Portanto, em um ambiente RIP-1 com VLSMs, mensagens Destination Unreachable (ICMP tipo 3, código 0) provavelmente trafegarão na rede. O ideal é que mensagens deste tipo não existam na rede.

6.10.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Você tem um problema de roteamento?

TESTE 2

TESTE 3

Existem VLSMs ou sub-redes descontinuadas em sua rede?

Verifique a tabela de rotas dos roteadores ligados a sub-redes com máscara variável ou que ligam redes descontinuadas.

Teste confirmatório 1

É provável que os usuários das redes prejudicadas reclamem. Conecte-se em uma máquina de uma das redes atingidas pelo problema e direcione um `traceroute` para uma máquina na outra rede.

Se o seu teste revelar que faltam rotas nos roteadores (!H na saída do `traceroute`) ou que os datagramas estão seguindo por um caminho inesperado você realmente está com problema de roteamento e o teste confirmatório 2 deve ser realizado. Caso contrário, a falta de conectividade observada é provavelmente devido a erros em camadas superiores.

Teste confirmatório 2

Como gerente da rede você deve conhecer o caminho que o datagrama deve seguir entre cada uma das sub-redes. Neste caminho existem redes não contíguas ou sub-redes com máscaras diferentes (VLSMs)? Uma documentação de rede atualizada vai ajudar a responder esta questão. Tendo encontrado máscaras distintas para sub-redes ou redes descontinuadas, o problema está confirmado. Caso a documentação da rede não esteja atualizada, segue abaixo algumas dicas de como confirmar mais rapidamente este problema.

Como os demais problemas RIP apresentados, este problema passa a existir quando alguma mudança é efetuada na rede. Se nada foi modificado na rede e de repente surgirem reclamações, você tem um problema, mas não este!

Se antes tudo funcionava bem e após uma modificação problemas passaram a existir, comece a desconfiar do que foi modificado (lembre-se da metodologia apresentada no Capítulo 3). Abaixo são listadas algumas situações que podem levar a este problema.

1) você acrescentou uma nova sub-rede em um ambiente RIP-1 → a máscara desta nova sub-rede não tem o mesmo comprimento das máscaras das demais sub-redes;

2) você está reavaliando a utilização dos endereços IP da organização (que utiliza RIP-1) e resolveu modificar algumas

máscaras para um melhor aproveitamento de endereços → você não lembrou de manter fixo o comprimento das máscaras das sub-redes e de não configurar redes descontinuadas;

Verifique primeiro as últimas modificações realizadas! Se for descoberto que pelo menos uma máscara de sub-rede é diferente das demais ou que existem redes descontinuadas, o problema foi confirmado.

Se você tinha um ambiente onde as tabelas de rotas eram construídas estaticamente e está migrando para um ambiente RIP-1, você realmente terá que descobrir e certificar-se de que não existem VLSMs e redes descontinuadas. Verifique nos roteadores o endereço configurado em cada uma de suas interfaces e aproveite para organizar melhor a documentação de sua rede!

Após ter confirmado a existência de VLSMs e/ou redes descontinuadas com o teste confirmatório 2, se você ainda tiver dúvidas, pode realizar o seguinte teste:

Teste confirmatório 3

Verifique a tabela de rotas dos roteadores ligados a VLSMs ou redes não contíguas. No exemplo da Figura 6-7, você deveria analisar a tabela de rotas dos roteadores roteador4 e roteador2, e verificaria que roteador4 não sabe como chegar na rede 128.128.6.0/24 e que roteador4 não sabe chegar em nenhuma das sub-redes, exceto na que está diretamente conectada a ele. Certifique-se de que a rota desejada realmente não está presente na tabela de rotas. Esta análise pode ser feita através de um terminal de gerência ou com o auxílio de uma estação de gerência SNMP. Veja **PROCEDIMENTO 11.3**.

6.10.5 Sugestões de tratamento

Para solucionar este problema o ideal seria adquirir roteadores que suportem RIP-2, ou mudar de protocolo e passar a utilizar OSPF, por exemplo, para a construção dinâmica das tabelas de rotas.

Caso nenhuma destas soluções seja possível e RIP-1 tenha realmente que ser utilizado, você ainda tem duas saídas:

- modificar as máscaras das sub-redes para um valor único em toda a rede;
- configurar algumas rotas estáticas em seus roteadores de forma que o problema seja solucionado. Por exemplo, na Figura 6-7, você poderia

inserir em roteador4 rotas estáticas para as sub-redes 128.128.1.0/24, 128.128.2.0/24, 128.128.3.0/24, 128.128.4.0/24, 128.128.5.0/24 e 128.128.8.0/24.

6.11 Diâmetro RIP com mais de 15 roteadores

6.11.1 Descrição

Leia mais sobre RIP no apêndice 8

O protocolo RIP limita o diâmetro máximo de uma rede a 15 roteadores. Isto é, em um ambiente RIP, duas redes só conseguem se comunicar se existirem menos de 16 roteadores no caminho entre elas. Essa limitação se deve ao fato de que um valor de métrica específico deveria ser escolhido para indicar um destino inalcançável, e o valor 16 foi escolhido. Este problema não ocorre com freqüência, pois é necessário que a rede possua um diâmetro de 16 roteadores entre duas sub-redes, não sendo esta uma topologia comum.

Considere a rede apresentada na Figura 6-8. Observe que roteador15 anunciará a roteador16 que chega na LAN do Departamento de Produção com métrica 15. Roteador16 adicionará 1 a este valor, pois ele está a uma distância de 1 *hop* de roteador15 e considerará a LAN do Departamento de Produção inalcançável e não incluirá a rota em sua tabela de roteamento. Desta forma, as máquinas da LAN do Departamento de Produção não conseguem de comunicar com as máquinas do Almoxarifado. O mesmo ocorre em roteador1 em relação à LAN do Almoxarifado.

Nas configurações mais simples do RIP, é comum usar métricas que simplesmente informam quantos roteadores o datagrama irá atravessar até chegar no destino (*hop counts*). Em configurações mais complexas, uma métrica pode ter outros significados, como por exemplo, o custo de enviar datagramas por determinados caminhos, ou o atraso sofrido, etc. Nestes casos, é possível que métricas de valor 16 sejam atingidas mesmo que o diâmetro máximo da rede não chegue a este valor.

Leia mais sobre endereçamento no apêndice 7

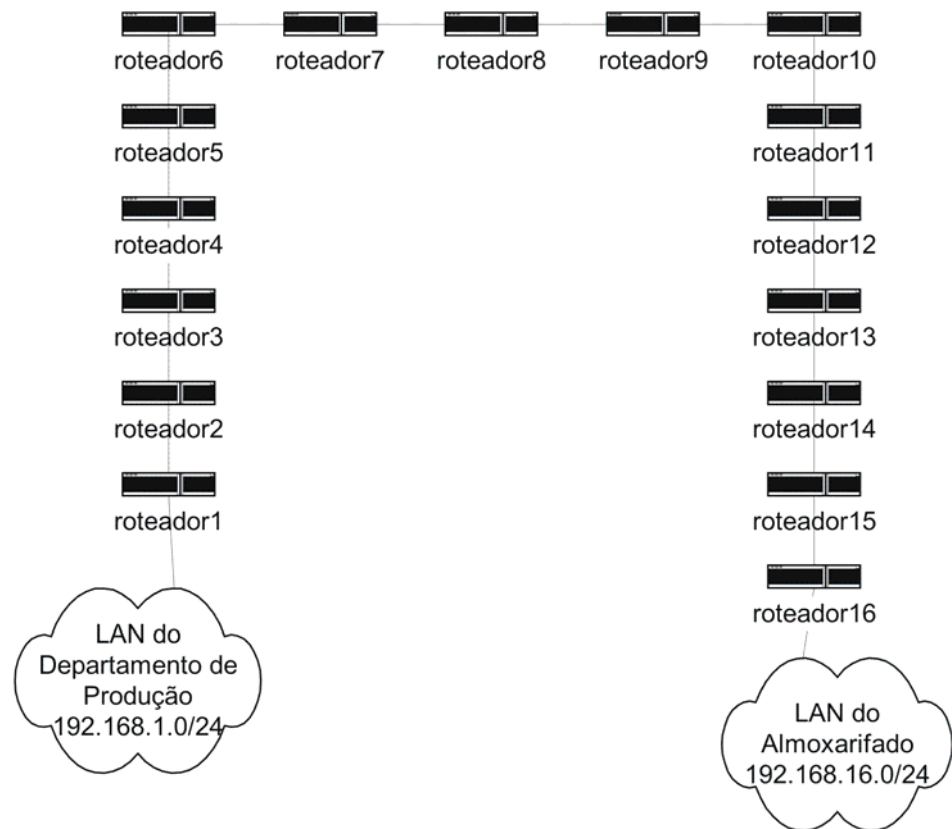



Figura 6-8: exemplo de rede com distância maior que 15 entre duas sub-redes

6.11.2 Sintomas

Os usuários das redes envolvidas irão reclamar de falta de conectividade entre as redes. No exemplo apresentado na seção anterior, os usuários do Departamento de Produção iriam reclamar que não conseguem acessar a aplicação de controle de estoque que está na LAN do Almoxarifado.

6.11.3 Sinais

Procedimento **11.10**

As rotas com métrica 16 não são anunciadas nem inseridas nas tabelas de rotas dos roteadores, tornando-as incompletas. Se existir rota default, ela será usada sempre que a rota específica para um certo destino não for encontrada. Se nenhuma rota default estiver configurada, o roteador não saberá para onde enviar o datagrama, sendo este descartado. Após descartar o datagrama, o roteador transmitirá uma mensagem ICMP Destination Unreachable para a máquina origem do datagrama. Portanto, em um ambiente RIP onde métricas 16 são encontradas, mensagens Destination Unreachable (ICMP tipo 3, código 0) provavelmente trafegarão na rede. O ideal é que mensagens deste tipo não existam na rede.

6.11.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1 — Analise o caminho seguido por um datagrama entre as duas redes. A partir de qual roteador o caminho é desviado ou não existem rotas?

TESTE 2 — Como está a tabela de rotas do roteador localizado no teste anterior? Sua tabela de rotas está realmente incompleta?

TESTE 3 — De acordo com a topologia da rede existem mais de 15 roteadores entre duas sub-redes?

Teste confirmatório 1

A conseqüência deste problema é a falta de conectividade entre duas ou mais redes. Ao suspeitar da existência de mais de 15 roteadores entre as redes, ou de métricas RIP superiores a 15, conecte-se em uma máquina de uma das redes envolvidas e direcione um `traceroute` a uma máquina da outra rede envolvida.

Considere novamente o exemplo ilustrado na Figura 6-8. O gerente do Departamento de Produção liga para o gerente de redes e diz que desde o dia anterior não consegue utilizar a aplicação de controle de estoque. O gerente de redes sabe que esta aplicação está implantada no Almoxarifado, e começa a realizar seus testes para descobrir e confirmar o problema. No dia anterior o roteador5 foi adicionado na rede, e o gerente de redes desconfia que a distância entre as duas redes tornou-se 16 *hops*. Ele se conecta em uma máquina do Departamento de Produção e direciona um `traceroute` para o BD do Almoxarifado.

A saída foi a seguinte:

```
# traceroute –n 192.168.16.2

1   0.132 ms   0.211 ms   0.217 ms   192.168.1.1

2   !H   !H   !H
```

Esta saída indica que o roteador1 não sabe para onde enviar datagramas destinados à rede do Almoxarifado. Conectando-se em uma máquina do Almoxarifado e direcionando um `traceroute` para uma máquina do Departamento de Produção obtém-se uma saída semelhante:

```
# traceroute –n 192.168.1.2

1   0.132 ms   0.211 ms   0.217 ms   192.168.16.1
```

```
2   !H   !H   !H
```

Isto significa que o roteador16 também não possui rota para a rede 192.168.1.0/24 (LAN do Departamento de Produção).

Este teste serve também para negar a existência deste problema. Se o roteador1 conhecesse a rota para a rede 192.168.16.0/24, e mais adiante um outro roteador – por exemplo, o roteador5 – estivesse com sua tabela de rotas incompleta, o problema não seria o apresentado neste capítulo.

Se existirem rotas *default* nos roteadores elas serão utilizadas, e, neste caso, ou a rota *default* coincidirá com a rota que deveria ser seguida ou o datagrama começará a caminhar por um caminho incorreto. No primeiro caso, é até possível que uma grande coincidência faça com que o problema não seja percebido. Considere, por exemplo, que a rota *default* do roteador1 é o roteador2, e que a rota *default* do roteador16 é o roteador15. Neste caso, apesar das redes estarem a mais de 15 *hops* de distância, elas continuarão se comunicando. No segundo caso, é simples deduzir que não existe rota para o destino especificado e que a rota *default* está sendo utilizada.

Teste confirmatório 2

Observe a tabela de rotas do roteador a partir do qual o caminho foi desviado ou não existe rota. Certifique-se de que a rota desejada realmente não está presente na tabela de rotas, que o RIP está habilitado e funcionando apropriadamente. Esta análise pode ser feita através de um terminal de gerência ou com o auxílio de uma estação de gerência SNMP. Veja procedimento apresentado na Seção 11.3.

Teste confirmatório 3

Analise a topologia de sua rede. Se você usa RIP e existem mais de 15 roteadores entre duas sub-redes, o problema está confirmado. Se a documentação da topologia da rede estiver desatualizada, o `traceroute` pode novamente auxiliar na confirmação do problema.

Considere novamente o exemplo da Figura 6-8. O gerente da rede não está bem certo sobre o caminho que os datagramas devem percorrer ao saírem da LAN do Departamento de Produção para a LAN do Almoxarifado. Mas ele sabe que, saindo da LAN do

Departamento de produção, o datagrama deve passar por roteador1 e logo após por roteador2 e roteador3. O gerente, então, conectou-se via `telnet` ou através de um terminal de gerência em roteador2, que é o segundo roteador pelo qual o datagrama deveria passar. Dele, o gerente direcionou um `traceroute` para uma máquina da LAN do Almoxarifado. A saída do `traceroute` foi a seguinte:

```
# traceroute –n 192.168.16.2

1   0.132 ms   0.211 ms   0.217 ms   192.168.3.1

2   0.231 ms   0.165 ms   0.153 ms   192.168.4.1

3   0.214 ms   0.189 ms   0.344 ms   192.168.5.1

4   0.254 ms   0.213 ms   0.222 ms   192.168.6.1

5   0.235 ms   0.198 ms   0.210 ms   192.168.7.1

6   0.301 ms   0.255 ms   0.278 ms   192.168.8.1

7   0.226 ms   0.209 ms   0.245 ms   192.168.9.1

8   0.219 ms   0.159 ms   0.218 ms   192.168.10.1

9   0.132 ms   0.211 ms   0.217 ms   192.168.11.1

10  0.231 ms   0.165 ms   0.153 ms   192.168.12.1

11  0.214 ms   0.189 ms   0.344 ms   192.168.13.2

12  0.231 ms   0.199 ms   0.243 ms   192.168.14.1

13  0.231 ms   0.229 ms   0.235 ms   192.168.15.1

14  0.301 ms   0.302 ms   0.265 ms   192.168.16.1

15  0.282 ms   0.209 ms   0.287 ms   192.168.16.2
```

Este resultado informa que entre roteador2 e a LAN do Almoxarifado existem 14 roteadores. Somando o roteador1 e o roteador2, obtêm-se 16 roteadores entre as duas LANs e o problema está então confirmado.

Se você ou sua equipe de gerência modificou os custos de suas interfaces e as métricas RIP não equivalem ao número de roteadores entre duas redes, verifique se a soma dos custos RIP entre as duas redes envolvidas leva a métricas maiores que 15. Se levar o problema foi confirmado.

6.11.5 Sugestões de tratamento

Se as métricas utilizadas em cada interface já estão configuradas com valor 1, duas soluções são possíveis:

- reprojetar a rede de forma que entre duas sub-redes não existam mais de 15 roteadores;
- passar a utilizar outro protocolo de roteamento interior, como OSPF, por exemplo.

Se os custos RIP tiverem sido modificados, reduza os valores de forma a não mais existirem métricas maiores que 15.

Se as métricas RIP foram modificadas e não indicam o número de roteadores entre duas redes, mais interessante que reduzir as métricas seria passar a utilizar outro protocolo de roteamento interno, baseado em um algoritmo de estado de enlace, como OSPF, por exemplo.

Idealmente, uma estação de gerência oferece o serviço de descobrimento automático de topologia. Com o descobrimento automático, a documentação da topologia da rede não ficará desatualizada. O protocolo de descobrimento de topologia Cisco (Cisco Discovery Protocol – CDP) pode ser utilizado em conjunto com SNMP com a finalidade de descobrir automaticamente quem são os vizinhos de um equipamento. O protocolo CDP pode ser ativado em todos os equipamentos da Cisco. As informações descobertas são representadas por objetos da CISCO-CDP-MIB, podendo ser obtidas via SNMP. Se a estação de gerência oferecer o serviço de descobrimento automático de topologia, a adição de novos roteadores será rapidamente percebida.

6.12 Roteadores RIP-2 não enviam ou recebem pacotes RIP-1

6.12.1 Descrição

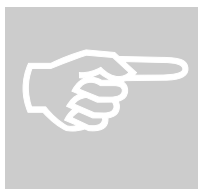
Leia mais sobre RIP no apêndice 8

Este problema só poderá ocorrer se, em uma rede, alguns roteadores já suportam RIP-2 e outros ainda permaneçam implementando apenas RIP1. Geralmente, por *default*, as interfaces de um roteador RIP-2 são configuradas para: 1) receber pacotes RIP-1 e RIP-2[32] e 2) enviar pacotes RIP-2 através do endereço de difusão. No entanto, esta configuração pode ser alterada. Veja algumas situações que causarão problemas:

[32] Mensagens RIP-2 têm o mesmo formato de mensagens RIP. A única diferença entre elas é que as mensagens RIP-2 usam octetos não utilizados do campo de endereço das mensagens RIP1 para enviar a máscara da sub-rede.

- se os nós que implementam RIP-2 forem configurados para anunciar suas rotas através do endereço *multicast* 224.0.0.9, os nós RIP-1 não receberão essas atualizações de roteamento. Estes roteadores só recebem mensagens RIP destinadas ao endereço de difusão. Isto causará tabelas de rotas incompletas;

- os roteadores RIP-2 podem ser configurados para receber apenas pacotes RIP-2 via endereço de *multicast*. Sendo assim, eles não receberão os pacotes RIP-1, que são transmitidos para o endereço de difusão.

Na Figura 6-9, o roteador1 implementa RIP-2, enquanto os demais implementam RIP-1. As configurações *default* de roteador1 foram modificadas, e ele só envia e recebe pacotes RIP-2 (usando endereço de *multicast*). Os anúncios enviados por roteador1 não serão recebidos por roteador2 e roteador3, e, conseqüentemente, eles não saberão como rotear pacotes destinados à LAN do Setor de Vendas. Da mesma forma, roteador1 não considerará os anúncios de rotas do roteador2 e do roteador3.

Em um ambiente misto, é necessário ter em mente que todas as limitações do RIP-1 (não suportar VLSM e *supernetting*, por exemplo) devem ser consideradas.

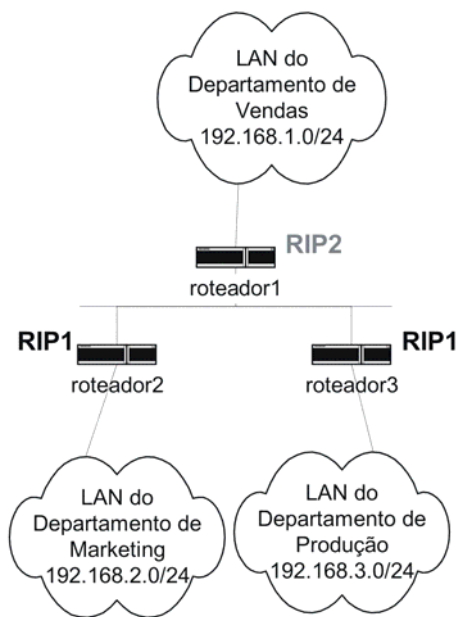



Figura 6-9: ambiente misto, com dois roteadores RIP-1 e um roteador RIP-2

6.12.2 Sintomas

Os usuários reclamarão de falta de conectividade para uma ou mais redes. No exemplo apresentado anteriormente, os usuários da LAN do Departamento de Vendas reclamarão que não conseguem acessar as páginas dos demais departamentos. Ou ainda, os usuários do Departamento de Marketing se chatearão por não estarem conseguindo ver as estatísticas de venda da empresa.

6.12.3 Sinais

Procedimento

11.10

Os nós RIP-1 não receberão as informações de roteamento anunciadas pelos nós RIP-2 que estiverem utilizando endereçamento multicast. É possível também que os nós RIP-2 não estejam aceitando os pacotes RIP-1 enviados por difusão. Portanto, as tabelas de rotas dos roteadores ficarão incompletas. Se existir rota default, ela será usada sempre que a rota específica para um certo destino não for encontrada. Se nenhuma rota default estiver configurada, o roteador não saberá para onde enviar o datagrama, sendo este descartado. Após descartar o datagrama, o roteador transmitirá uma mensagem ICMP de destino inalcançável para a máquina origem do datagrama. Portanto, em um ambiente RIP misto onde os nós RIP-2 só enviam e recebem pacotes RIP-2 através de endereçamento multicast, mensagens ICMP de destino inalcançável (ICMP tipo 3, código 0) provavelmente trafegarão na rede. O ideal é que mensagens deste tipo não existam na rede.

6.12.4 Testes confirmatórios

Este é um problema de configuração, e não vai ocorrer sem que algo esteja sendo modificado na rede. Portanto, sempre que, em um ambiente RIP misto, um novo nó RIP estiver sendo inserido ou as configurações RIP estiverem sendo alteradas, alguns cuidados devem ser tomados. Ver a Seção **SUGESTÕES DE TRATAMENTO**. Alterações que tornem o ambiente RIP misto também devem ser executadas com cautela.

TESTE 1

Localize os roteadores com maior probabilidade de estarem mal configurados;

TESTE 2

Verifique que tipo de pacote RIP as interfaces destes roteadores aceitam receber e para que endereço elas enviam mensagens RIP;

Teste confirmatório 1

Neste teste você vai procurar quais são os roteadores que estão enviando e/ou recebendo apenas pacotes RIP-2 via *multicast*. Estes roteadores ficam sob suspeita e devem passar pelo teste confirmatório 2.

Apenas roteadores RIP-2 podem ficar sob suspeita. Isto ocorre porque apenas eles são capazes de enviar e receber pacotes RIP-1 e RIP-2. Já os nós RIP-1 só sabem falar RIP-1 mesmo; não há, portanto, o que ser configurado.

Comumente, ambientes RIP-1 vão sendo atualizados para se tornar ambientes RIP-2 através da substituição de roteadores RIP-1 por roteadores que suportem RIP-2, ou através da inserção de novos roteadores que já suportem a mais nova versão do protocolo RIP. Neste caso, o novo roteador RIP-2 fica sob suspeita.

Num caso mais raro, em que o ambiente era completamente RIP-2 e um novo roteador RIP-1 teve que ser inserido, os antigos roteadores RIP-2 é que ficam sob suspeita.

Por fim, o gerente da rede pode configurar que tipo de pacote RIP as interfaces de seu roteador RIP-2 irão enviar e processar (ver Seção **SUGESTÕES DE TRATAMENTO**). Se estas configurações foram alteradas em um roteador, este fica sob suspeita.

Para ilustrar esta busca, observe novamente o exemplo da Figura 6-9. Considere que roteador1 e roteador2 já existiam, e que roteador3 foi adicionado à rede. Esta situação não leva a problema algum (exceto se ele já existia antes!), pois o ambiente já era misto e um roteador RIP-1 foi inserido.

Considere agora que roteador2 e roteador3 (ambos suportam apenas RIP-1) já existiam na rede, e que roteador1 (que implementa RIP-2) foi adicionado para incluir na rede da empresa a LAN do Departamento de Vendas. Diante deste quadro, roteador1 torna-se suspeito e deve ter a sua configuração RIP analisada, como mostra o teste confirmatório a seguir.

Teste confirmatório 2

Examine que tipos de pacotes RIP as interfaces dos roteadores sob suspeita estão configuradas para enviar e receber. Esta análise pode ser feita de duas formas:

1. Através de uma interface de linha de comando

Os comandos a serem executados irão depender do fabricante e do modelo do roteador em questão.

Em alguns roteadores Cisco, por exemplo, os comandos a seguir apresentam na tela os tipos de pacotes enviados e aceitos pela interface:

```
roteador> show ip rip send version

roteador> show ip rip receive version
```

O comando seguinte mostra toda a configuração corrente do roteador e pode também ser utilizado:

```
roteador# show running-config
```

2. Com o auxílio de uma estação de gerência SNMP

Duas variáveis da tabela rip2IfConfTable (extensões da MIB RIP versão 2 [RFC 1724]) auxiliarão esta análise: rip2IfConfSend e rip2IfConfReceive. Nesta tabela existe uma entrada para cada interface RIP do roteador. O objeto rip2IfConfSend informa que tipo de pacote RIP o roteador envia pela interface em questão. Alguns valores possíveis são:

- doNotSend (1) → nenhum pacote RIP é enviado pela interface;
- ripVersion1 (2) → envia atualizações RIP compatíveis com a RFC 1058 (especificação do RIP-1);
- rip1Compatible (3) → envia atualizações RIP-2 através do endereço de difusão;
- ripVersion2 (4) → envia atualizações RIP-2 através de endereço de *multicast*;

Se em alguma interface que se comunica diretamente com pelo menos um nó RIP-1 o valor ripVersion2 for encontrado o problema (ou parte dele) foi confirmado.

O objeto rip2IfConfReceive indica que versões de atualizações RIP são aceitas pela interface. Quatro valores são possíveis: rip1 (1), rip2 (2), rip1OrRip2 (3) ou doNotReceive (4). Se o valor rip2 for encontrado em interfaces que se comunicam diretamente com pelo menos um nó RIP-1, o problema foi confirmado.

6.12.5 Sugestões de tratamento

Este problema pode ser corrigido de duas formas:

- compre roteadores que implementem RIP-2 e torne seu ambiente completamente RIP-2;
- configure os roteadores RIP-2 para enviarem atualizações de roteamento para o endereço de difusão e aceitarem pacotes RIP-1 destinados ao endereço de difusão.

Esta configuração, mais uma vez, pode ser realizada de duas formas:

ATRAVÉS DE UMA INTERFACE DE LINHA DE COMANDO

Os comandos a serem executados dependem do fabricante e do modelo do roteador. Em um roteador Cisco, por exemplo, a configuração correta das interfaces diretamente conectadas a nós RIP-1 pode ser realizada, por exemplo, com os seguintes comandos:

```
roteador1# ip rip send version 1 2
```

```
roteador1# ip rip receive version 1 2
```

Também é possível escolher aceitar receber ou enviar apenas pacotes RIP-1.

```
roteador1# ip rip send version 1
roteador1# ip rip receive version 1
```

COM O AUXÍLIO DE UMA ESTAÇÃO DE GERÊNCIA SNMP

As variáveis rip2IfConfSend e rip2IfConfReceive da tabela rip2IfConfTable devem ter seu valor modificado da seguinte forma nas interfaces que estão diretamente conectadas a nós RIP-1:

- o valor da variável rip2IfConfSend deve ser modificado para o valor rip1Compatible;
- o valor da variável rip2IfConfReceive deve ser configurado com o valor rip1OrRip2.

6.13 Tráfego RIP saturando largura de banda

6.13.1 Descrição

Leia mais sobre RIP no apêndice 8

Periodicamente (de 30 em 30 segundos), cada roteador RIP envia uma cópia de sua tabela de rotas para todos os outros roteadores diretamente conectados a ele. Uma tabela de rotas contém uma entrada para cada rede da organização com a qual o roteador possa se comunicar direta ou indiretamente. Desta forma, a quantidade de informação enviada por um roteador é diretamente proporcional à quantidade de redes interligadas na organização. Sendo assim, dependendo da quantidade de redes e da capacidade dos enlaces, é possível que o volume de tráfego RIP seja tão grande que chegue a saturar os enlaces com menor largura de banda.

Considere, por exemplo, a rede da Figura 6-10. Considere também que cada um dos roteadores apresentados nela (exceto os roteadores da clínica e rt-creche), em média, está conectado direta ou indiretamente a 350 outras redes. Nesta inter-rede existem portanto, 22x350 = 7700 redes. Isto significa que na tabela de rotas dos roteadores, existem pelo menos 7700 entradas. Como os roteadores estão com o protocolo RIP ativado, a cada 30 segundos cada roteador envia para os roteadores diretamente conectados a ele informações de roteamento que consistem, nada mais nada menos, nas 7700 entradas de toda a sua tabela de rotas. Se você fizer os cálculos desconsiderando os dados de controle da camada de enlace, chegará à seguinte conclusão: a cada 30 segundos um roteador envia 163,8 KB de dados para os demais roteadores ligados a ele. Isto resulta em um tráfego médio de aproximadamente 43,7 Kbps. Quase 70% da largura de banda do enlace entre rt-14 e rt-clinica está sendo gasto com informações do protocolo RIP, consumindo praticamente toda a largura de banda do enlace que liga a rede do hospital da empresa à rede da empresa. Se rt-creche estivesse falando RIP com os demais roteadores, o enlace rt-8 ⇔ rt-creche também estaria congestionado devido ao tráfego RIP.

6.13.2 Sintomas

Os usuários reclamarão de rede lenta. Os médicos e funcionários da clínica apresentada na Figura 6-10 reclamariam de rede lenta e todas as aplicações hospedadas na clínica apresentariam um tempo de resposta muito grande se utilizadas fora dela.

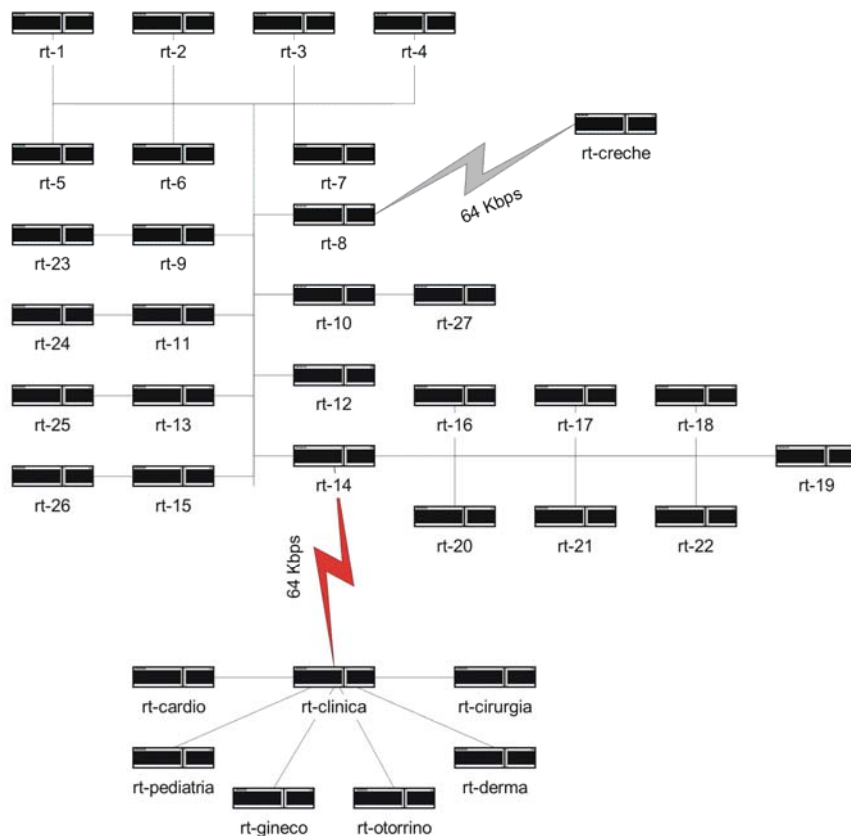



Figura 6-10: Inter-rede com 7700 redes conectadas por roteadores.

6.13.3 Sinais

Procedimento
10.10

Taxa de utilização de enlaces de longa distância[33] superior a 70%. A razão da preocupação com altas taxas de utilização é que após uma certa taxa de utilização, um pequeno aumento da utilização implica em um grande aumento do tempo de resposta.

6.13.4 Testes confirmatórios

RESUMO DOS TESTES

[33] Enlaces de redes locais, têm maior capacidade, não sendo provável a sua saturação devido ao tráfego RIP.

TESTE 1

Quantas redes estão interligadas? Milhares? Existem enlaces de baixa velocidade?

TESTE 2

Qual o tráfego RIP gerado pelos roteadores?

Teste confirmatório 1

Muito provavelmente os usuários reclamarão de rede lenta. Se a rede foi crescendo aos poucos, a percepção de rede lenta por parte dos usuários foi também aumentando aos poucos, até chegar a um ponto insuportável. Se a sua ferramenta de gerência estiver apresentando dados como tempo de `ping`, por exemplo, você notará o aumento gradual desta estatística se compará-la aos seus valores antigos.

A documentação da rede poderá ajudar a responder às seguintes questões:

- Quantas redes estão interligadas em sua inter-rede?
- Existem roteadores RIP ligados a enlaces de baixa velocidade em sua inter-rede?

Se em sua inter-rede existem mais de 8 mil redes interligadas, e se existem também enlaces de baixa capacidade, como 64 kbps, por exemplo, comece a desconfiar deste problema. Se necessário conecte-se nos roteadores ligados a enlaces de baixa capacidade e verifique o tamanho de suas tabelas de rotas. O procedimento apresentado na Seção 11.3 ensina como obter tabela de rotas de roteadores.

Em um roteador Linux você pode descobrir facilmente quantas entradas existem na tabela de rotas com o comando:

```
# netstat –nr | wc -l
```

Teste confirmatório 2

Para descobrir quanta largura de banda o tráfego RIP está consumindo, substitua a variável `n-entradas` da equação abaixo pelo número de entradas RIP nas tabelas de rotas dos roteadores.

A quantidade aproximada de tráfego RIP gerada por um roteador é[34]:

Tráfego de 1 roteador = (n-entradas x 4256) bps
25 x 30

Onde: 4256 é a quantidade de bits em um datagrama que contém uma mensagem RIP com anúncio para 25 redes, que é o máximo permitido por mensagem RIP.

Utilizando a equação acima você pode descobrir o tráfego RIP de um enlace. Se ele estiver muito alto o problema foi confirmado.

Na realidade, não é uma boa prática de gerência que você permita que mais de 5% da capacidade de um enlace seja desperdiçada com informações de roteamento. O ideal, portanto, é que de tempos em tempos, você monitore a quantidade largura de banda usada para o tráfego de informações de roteamento nos enlaces mais lentos.

6.13.5 Sugestões de tratamento

Protocolos baseados no algoritmo vetor-distância – como é o caso do RIP – têm a seguinte desvantagem: a cada 30 segundos cada roteador tem que enviar para os demais roteadores conectados diretamente a ele toda a sua tabela de rotas, tendo ela sofrido ou não modificações. Por outro lado, protocolos baseados no algoritmo de estado de enlace, como é o caso do OSPF, não trazem esta desvantagem. Os roteadores OSPF trocam apenas informações de roteamento que sofreram modificações. A melhor solução em longo prazo para este problema seria passar a usar um protocolo baseado no algoritmo de estado de enlace. OSPF é o mais utilizado atualmente.

Caso você não ache esta solução factível, poderá aumentar a largura de banda do enlace, isto é, em vez de pagar por um enlace de 64 Kbps, passe a pagar por um de 128 Kbps.

6.14 Filtro IP não permite a passagem de tráfego RIP (UDP 520)

6.14.1 Descrição

É possível que filtros de pacotes IP estejam configurados nos roteadores que implementam RIP. Os roteadores RIP trocam informações de roteamento

[34] Na realidade, o tráfego RIP gerado é um pouco maior, pois estes cálculos estão desconsiderando os gastos com dados de controle da camada de enlace.

através da porta UDP 520. Se existirem filtros IP barrando a entrada ou a saída de dados nesta porta, os roteadores RIP não poderão trocar as informações de roteamento, causando tabelas de rotas incompletas.

Para exemplificar este problema, considere a rede apresentada na Figura 6-11. Note que um filtro IP está configurado em roteador1. Este filtro não está permitindo a passagem do tráfego UDP 520 entre os roteadores roteador1 e roteador2. Portanto, os roteadores roteador2 e roteador3 não saberão como encaminhar pacotes destinados à LAN do Departamento de Finanças, e roteador1 não saberá chegar às demais LANs da empresa.

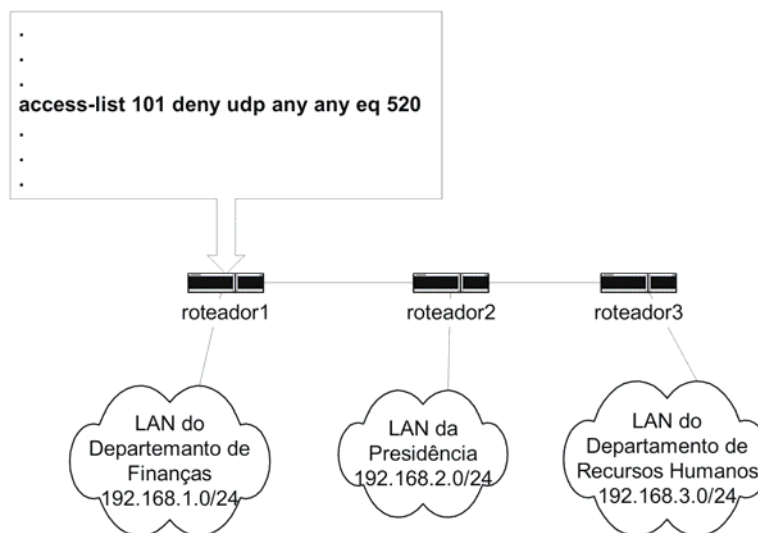



Figura 6-11: Ambiente RIP com filtro IP configurado no roteador1

6.14.2 Sintomas

Os usuários reclamarão de falta de conectividade para uma rede, várias redes ou todas as outras redes. No exemplo anterior, certamente, o pessoal de finanças reclamará que a rede só funciona internamente (falta de conectividade para todas as demais redes) e é provável que os diretores da empresa fiquem bastante chateados por não estarem conseguindo utilizar a aplicação de controle financeiro (falta de conectividade para uma rede) ou consultar o cadastro dos funcionários.

6.14.3 Sinais

Procedimento
11.10

Quando filtros de pacotes barram a passagem do tráfego RIP, as tabelas de rotas dos roteadores (que dependem desta troca de informações) ficarão incompletas. Se existir rota default, ela será usada sempre que a rota específica para um certo destino não for encontrada. Se nenhuma rota default estiver configurada, o roteador não saberá para onde enviar o datagrama, sendo este descartado. Após descartar o datagrama, o roteador transmitirá uma mensagem ICMP Destination Unreachable para a máquina origem do datagrama. Portanto, em um ambiente RIP onde existem filtros de pacotes que barram o tráfego UDP na porta 520,

mensagens Destination Unreachable (ICMP tipo 3, código 0) provavelmente trafegarão na rede. O ideal é que mensagens deste tipo não existam na rede.

Procedimento
11.9

Sendo roteados com base nas tabelas incompletas dos roteadores, laços lógicos podem ser formados. A formação dos laços vai levar à existência de mensagens ICMP de TTL excedido na rede. Idealmente estas mensagens não devem ser encontradas.

6.14.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Localize os roteadores nos quais filtros de pacotes estão configurados;

TESTE 2

Verifique se a saída e entrada de tráfego UDP na porta 520 são permitidos pelos filtros.

Teste confirmatório 1

Este, assim como os demais problemas RIP apresentados neste livro, é um problema de configuração. Neste caso porém, o problema não é de configuração do RIP, mas do filtro IP de um roteador que implementa RIP. Caso um filtro IP seja configurado em um roteador e este filtro esteja barrando o tráfego UDP na porta 520, após, no máximo, 180 segundos da ativação do filtro, as tabelas de rotas dos roteadores ficarão incompletas.

Portanto, se ao configurar filtros IP em um ambiente RIP o os sintomas e/ou sinais descritos anteriormente forem percebidos, considere a possibilidade do tráfego RIP estar sendo barrado. Localize os roteadores onde filtros IP foram configurados e ativados ultimamente e realize neles o teste confirmatório 2.

Teste confirmatório 2

Examine a configuração do filtro IP em cada roteador selecionado no teste confirmatório 1. Os comandos a serem executados dependem do fabricante e do modelo do roteador em questão.

Em um roteador Cisco, utilize o comando `show access-list` para analisar todas as listas de acesso configuradas.

Em um roteador Linux o comando para a criação e visualização das regras configuradas depende do pacote de filtragem instalado.

Atualmente, o filtro é configurado com um dos seguintes comandos: `iptables`, `ipchains` ou `ipfwadm`. Os comandos abaixo mostram as regras de entrada e de saída para configurações realizadas com `iptables`, `ipchains` e com `ipfwadm`.

```
# iptables –L –n | more

# ipchains –L -n| more

# ipfwadm –L –n | more
```

Caso exista uma regra que não esteja permitindo a entrada ou a saída de tráfego UDP na porta 520, o problema foi confirmado.

6.14.5 Sugestões de tratamento

O filtro IP de um roteador RIP, qualquer que seja a versão do protocolo RIP, deve sempre permitir a entrada e a saída de tráfego UDP na porta 520. Ao confirmar o problema modifique as regras do filtro para permitir a passagem do tráfego RIP.

Em um roteador Cisco, as regras de filtragem são configuradas através de comandos `access-list`. Considerando que os roteadores do exemplo apresentado na Seção **DESCRIÇÃO** são fabricados pela Cisco, o problema é solucionado com os seguintes comandos:

```
roteador1# no access-list 101 deny udp any any eq 520
roteador1# access-list 101 permit udp 192.168.4.1 0.0.0.0 any eq 520
roteador1# access-list 101 permit udp 192.168.4.2 0.0.0.0 any eq 520
```

O primeiro comando serve para negar a regra antes configurada que barrava o tráfego RIP. O segundo comando permite a transmissão de pacotes RIP de roteador1 para qualquer destino. O último comando permite que roteador1 aceite o tráfego RIP proveniente de roteador2. Uma regra mais genérica (e mais insegura) que poderia substituir as duas últimas regras é:

```
roteador1# access-list 101 permit udp 192.168. 0.0.255.255 any eq 520
```

A regra resultante do comando acima indica que é permitida a passagem de tráfego UDP na porta 520 de qualquer fonte para qualquer destino.

Se roteador1 fosse um Linux, e a interface que o liga a roteador2 fosse eth1, um dos seguintes conjuntos de regras deveria ser adicionado ao arquivo de configuração do filtro IP:

```
/sbin/ipchains –A input –p udp –s 192.168.4.1/32 –d 0/0 520 –i eth1 –j
ACCEPT

/sbin/ipchains –A output –p udp –s 192.168.4.2/32 –d 0/0 520 –i eth1 –j \
ACCEPT
```

ou

```
/sbin/ipfwadm –I –a accept –P udp –S 192.168.4.2/32 –D 0/0 520
/sbin/ipfwadm –O –a accept –P udp –S 192.168.4.1/32 –D 0/0 520
```

Em um filtro IP menos seguro os endereços das interfaces poderiam ser trocados por 0/0.

6.15 Referências

6.15.1 Recursos online (Internet)

[VLAN-REPORT] The Virtual LAN Technology Report.

http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf

[CISCO-DESIGN] Designing Switched LAN Internetworks.

http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2012.htm

[CISCO-RIP-BEHAVIOR] Behavior of RIP and IGRP When Sending and Receiving Updates.

http://www.cisco.com/warp/public/105/54.html

[CISCO-RIP-DISCONTIGUOUS] Why Doesn't RIP or IGRP Support Discontiguous Networks?

http://www.cisco.com/warp/public/105/55.html

[CISCO-RIP-VLSM] Why Don't RIP and IGRP Support Variable-Length Subnet Mask?

http://www.cisco.com/warp/public/105/53.html

[CISCO-VLAN-TRUNKS] CONFIGURING ETHERNET VLAN TRUNKS. http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/e_trunk.htm

[DHCP_FAQ] Wobus, J., Lemon, T., Droms, R. DHCP FAQ.

http://www.dhcp-handbook.com/dhcp_faq.html

6.15.2 RFCs

[RFC 1724] Malkin, G., Baker, F. RIP Version 2 MIB Extension. Novembro, 1994.

[RFC 2453] Malkin, G. RIP Version 2. Novembro, 1998.

6.15.3 Livros base

[COMER] Comer, D. Internetworking with TCP/IP: Principles, Protocols, and Architectures. Volume 1. Quarta edição. Prentice Hall, 2000.

[CISCO-ROUTING-TCP/IP] Doyle, J. Routing TCP/IP, Volume 1: CCIE Professional Development. Cisco Press. Setembro, 1998.

[CISCO-IP-ROUTING] Sportack, M. IP Routing Fundamentals. Cisco Press. Fevereiro, 1999.

[DHCP-HANDBOOK] Lemon, T. Droms, R. The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services. Pearson Higher Education. Outubro, 1999.

[DHCP-WIN-2000] Alcott, N. DHCP for Windows 2000. O'Reilly. Janeiro, 2001.

[PERF&FAULT-CISCO] Maggiora, P. L. D., Elliot, C. E., Pavone Jr, R. L., Phelps, K. J., Thompson, J. M. Performance and Fault Management. Cisco Press. 2000.

Capítulo

7

7 Problemas de nível de aplicação

Neste capítulo encontram-se 9 problemas que podem ocorrer em uma rede relacionados à camada de aplicação, em especial aos protocolos DNS (Domain Name Service) e SMTP (Simple Mail Transfer Protocol): O serviço de nomes não está habilitado, DNS: descasamento de registros A e PTR em arquivos de zonas, Inconsistência entre registros dos servidores DNS primário e secundários, O TTL default de uma zona DNS não está configurado, DNS: TTL e outros campos do registro SOA com valores inadequados, Falta "." após nomes totalmente qualificados em registros DNS, Filtro IP barrando tráfego DNS, Servidor de correio eletrônico com repasse totalmente aberto e Servidor de correio eletrônico com repasse totalmente fechado.

7.1 O serviço de nomes não está habilitado

7.1.1 Descrição

Aprenda mais sobre o serviço de nomes no apêndice 10

A implementação do serviço de nomes mais utilizada no mundo o BIND. Esta implementação é tipicamente executada em ambientes Unix-like. O programa servidor de nomes chama-se `named`. Outra implementação que já começa a ser bastante utilizada é a da Microsoft, que pode ser executada no Windows NT/2000 Server. Neste caso, o programa servidor chama-se `dns.exe`.

Se o servidor de nomes de sua organização não estiver em execução, o seu serviço de resolução de nomes não funcionará. O servidor de nomes é idealmente iniciado automaticamente durante a própria inicialização do sistema operacional onde o servidor está instalado.

Se, por exemplo, o programa `named` de um servidor de nomes primário não estiver em execução, um servidor de nomes secundário será utilizado pelos clientes (se estiver configurado neles). No entanto, quando o servidor secundário não consegue falar com o primário durante um certo tempo, ele desiste de ser secundário, e o serviço de nomes realmente não mais funcionará.

Se o servidor de nomes não estiver em execução nos servidores secundários, o domínio ficará sem servidor de nomes secundário, e nenhum servidor de nomes estará disponível quando houver algum problema com o servidor de nomes primário

A seguinte situação levaria a este problema: você atualiza o BIND para uma versão mais nova e o `named` é instalado em um diretório diferente do anterior (por exemplo, o `named` anterior estava em /usr/sbin e o novo está em /usr/local/bin). Além disso, para economizar o disco do seu servidor, você remove `named` anterior. Tudo estaria bem, se você não tivesse esquecido de um detalhe: modificar o arquivo de inicialização do sistema operacional onde o `named` é ativado para chamar o novo servidor. Apesar de não ser uma boa prática, após a atualização você pode iniciar o novo `named` manualmente. E assim é feito. Após um *boot* o serviço de nomes simplesmente não mais funcionará. Portanto, se você atualizar a versão do BIND para uma mais nova lembre-se de verificar se a nova versão vai ser iniciada automaticamente.

7.1.2 Sintomas

Geralmente, os usuários acessam os serviços da rede através dos nomes dos servidores. Por exemplo, ninguém navega através de endereços IP, e sim através de nomes. Qual o endereço IP do servidor Web da Cisco? Não sabe, não é? O *site* da Cisco é acessado através do nome do servidor Web: www.cisco.com. Na maioria das vezes, servidores são acessados através de seu nome, e não de seu endereço IP.

O mapeamento de um nome em um endereço IP e vice-versa é realizada pelos servidores de nomes. Se o servidor de nomes de sua organização não estiver em execução, a resolução não funcionará, e não será possível para seus usuários acessarem outras máquinas através de seus nomes. Todos os serviços acessados através dos nomes dos servidores ficarão indisponíveis. Durante a navegação, por exemplo, o próprio navegador alertará o usuários sobre o erro de DNS. Portanto, em geral, a reclamação dos usuários será de que a rede não está funcionando.

7.1.3 Sinais

Procedimento **11.10**

Imagine o que acontece quando o servidor de nomes não está ativado. Solicitações de resolução de nomes chegarão à porta UDP/53 e nenhum processo estará disponível para tratar a solicitação. Então a máquina destino enviará à máquina que solicitou o serviço uma mensagem ICMP *Port Unreachable* (tipo 3, código 3). Portanto, quando o serviço de nomes não estiver habilitado, os clientes receberão mensagens ICMP Port Unreachable sempre que tentarem utilizar o serviço de resolução de nomes.

Procedimento **11.14**

De todas as máquinas da rede, percebemos que há conectividade com outras máquinas através de seu IP, mas não através de seu nome.

7.1.4 Testes confirmatórios

RESUMO DOS TESTES

TESTE 1

Verifique se o processo servidor de nomes está em execução nos servidores de nomes primário e secundários;

TESTE 2

Certifique-se de que o servidor de nomes está sendo iniciado durante a inicialização da máquina servidora de nomes;

Teste confirmatório 1

Este teste confirmatório depende de que implementação do serviço de nomes está sendo utilizada. Como o BIND é a implementação mais utilizada no mundo, este teste considera apenas ela.

Os sinais/sintomas de falhas no serviço de nomes são bastante fortes e por isso elas são rapidamente localizadas, seja pelos administradores da rede, seja pelos usuários.

Na máquina servidora de nomes, verifique se o processo servidor de nomes está em execução. Em outras palavras, verifique se o `named` ou `dns.exe` está em execução.

Em um servidor Linux utilize o seguinte comando:

```
# ps –ae | grep named
```

No Windows NT e 2000 verifique quais os processos que estão em execução e verifique se o seu servidor de nomes (`dns.exe`) está no ar. Você pode ver os processos em execução pressionando as teclas CTRL + ALT + DEL simultaneamente e logo após pressionando o botão Gerenciador de Tarefas. Dentre outros dados, este gerenciador apresenta todos os processos em execução na máquina.

Se for constatado que o servidor de nomes não está em execução o problema foi confirmado parcialmente. Realize o teste confirmatório 2. Caso contrário, o problema foi negado. Estude melhor os sinais e sintomas do problema, é possível que existam erros nos arquivos de configuração do BIND (veja outros problemas relacionados ao serviço de nomes).

Teste confirmatório 2

Verifique se o processo `named` está sendo habilitado durante a inicialização da máquina servidora de nomes. Se não estiver o problema foi confirmado. Caso contrário, é provável que o `named` não execute devido a erros detectados nos seus arquivos de

configuração – em algumas versões do BIND o servidor pára a execução quando encontra erros nos arquivos de configuração.

Em máquinas Linux Slackware[35], geralmente o serviço de nomes é iniciado no arquivo /etc/rc.d/rc.inet2, onde todos os serviços básicos de rede são ativados. Certifique-se de que o named está sendo iniciado neste arquivo ou em outro arquivo. O seguinte comando irá lhe auxiliar nesta procura:

```
# grep named /etc/rc.d/rc*
```

Se os comandos que ativam o named estiverem comentados ou não existirem, o problema foi confirmado. Se o comandos que iniciam o named existem, e não estão comentados, verifique se o caminho para o processo named está correto. Se não estiver o problema foi confirmado. Caso contrário, é provável que o BIND não entre em execução por ter encontrado erros nos arquivos de configuração.

Em máquinas Linux baseadas no *System V* – como Red Hat, por exemplo – a verificação é um pouco diferente. Verifique se no diretório /etc/rc.d/rc3.d (ou rc5.d[36]) existe um *link* iniciado com a letra "S" que aponta para o arquivo /etc/rc.d/init.d/named.

```
# grep named /etc/rc.d/*/S*
```

Em seguida, verifique se o arquivo /etc/rc.d/init.d/named existe e se o servidor chamado é o correto.

Em um servidor Windows NT, no menu Iniciar, escolha: Configurações > Painel de Controle > Serviços. Surgirá uma janela que apresenta informações tais como estado atual (estão ou não em execução) e modo de inicialização (se é automática, manual ou se está desativada) sobre cada um dos serviços instalados. Se o servidor DNS não estiver sendo iniciado automaticamente, o problema foi confirmado. No Windows 2000, o Gerenciador de Serviços pode ser obtido da seguinte forma: no menu Iniciar, escolha: Programas > Ferramentas Administrativas > Serviços. O servidor DNS deve estar sendo iniciado automaticamente, caso contrário o problema foi confirmado.

---

[35] Inicialização parecida com o sistema BSD.

[36] Para as máquinas que trabalham em ambiente gráfico.

7.1.5 Sugestões de tratamento

Este é um problema de fácil e rápida solução, quando não está sendo causado por outro problema. Algumas versões do BIND não entram em execução quando encontram erros nos arquivos de configuração.

O serviço de nomes deve ser ativado durante a inicialização do servidor de nomes. Como você já percebeu, o arquivo que deve ser configurado para iniciar o named depende do sistema operacional que você está utilizando.

Em máquinas Linux Slackware, ative o named no arquivo /etc/rc.d/rc.inet2. Considere que o named está instalado no diretório /usr/sbin. Então as seguintes linhas no arquivo rc.inet2 poderiam ser adicionadas (ou "descomentadas"):

```
if [ -x /usr/sbin/named ]; then
echo -n " named "
/usr/sbin/named
fi
```

A partir do próximo *boot* o named será ativado automaticamente.

Se o named não estiver ativado no momento, ative-o com o seguinte comando:

```
# /usr/sbin/named
```

O caminho para o processo named pode ser outro, depende de onde o named está instalado[37]. Se você preferir reinicie a máquina para certificar-se de que o problema foi solucionado Após a ter reiniciado o servidor de nomes, verifique se ele está em execução:

```
# ps –ae | grep named
```

Se você atualizou o BIND para uma nova versão e o named foi instalado em um diretório diferente do diretório onde estava o named anterior, simplesmente corrija o caminho para o named no arquivo rc onde ele estiver sendo ativado. Em Linux Slackware isto será feito em /etc/rc.d/rc.inet2.

Em máquinas com inicialização baseada em *System V*, crie um link simbólico (cujo nome inicie com a letra "S") para /etc/rc.d/init.d/named no diretório /etc/rc.d/rc3.d[38]:

```
# cd /etc/rc.d/rc3.d
# ln -s S45named ../init.d/named
```

Você pode iniciar o servidor de nomes manualmente com o comando:

```
# /etc/rc.d/init.c/named start
```

---

[37] O comando `type named` irá lhe informar em que diretório o `named` está instalado.

[38] Se a máquina onde está seu servidor opera em ambiente gráfico, o link simbólico deve ser criado no diretório /etc/rc.d/rc5.d.

Em máquinas Windows NT, no menu Iniciar escolha Configurações > Painel de Controle > Serviços. Selecione o serviço "Servidor DNS" e pressione o botão Inicialização. Escolha o tipo de inicialização "Automática" e pressione OK. Se o servidor DNS não estiver em execução, pressione o botão Iniciar para ativá-lo manualmente. A partir do próximo *boot* o serviço de nomes será iniciado automaticamente.

Em máquinas com sistema operacional Windows 2000, no menu Iniciar escolha Programas > Ferramentas Administrativas > Serviços. Selecione o serviço Servidor DNS e pressione o botão direito do mouse sobre ele. Surgirá um menu. Nele escolha o item Propriedades. Surgirá uma janela que lhe permitirá configurar o tipo de inicialização para o serviço selecionado. Escolha "Automática". Se o serviço não estiver ativado no momento clique com o botão direito do mouse sobre ele e escolha Iniciar para ativá-lo manualmente. A partir do próximo *boot* ele será ativado automaticamente.

7.2 DNS: descasamento de registros A e PTR em arquivos de zonas

7.2.1 Descrição

Leia mais sobre DNS no apêndice 10

O serviço de nomes de domínio é responsável por realizar mapeamento direto – de um nome para um IP – e mapeamento reverso – de um IP para um nome. Infelizmente, no BIND[39] a configuração do mapeamento direto e reverso não é feita no mesmo registro, nem no mesmo arquivo de zona. É necessário um registro Internet Address (`IN A`) para o mapeamento direto e um registro Internet Pointer (`IN PTR`) para o reverso. Os registros `IN A` ficam no arquivo de zonas de mapeamento direto, enquanto os registros `IN PTR` ficam no arquivo de zona de mapeamento indireto. Por exemplo, para configurar que o IP da máquina pc-1.exemplo.com.br é 192.168.1.1 serão necessários dois registros. O registro seguinte deve ficar no arquivo de zona direto:

```
pc-1    IN     A      192.168.1.1    ; no arquivo de mapeamento direto
```

E o registro abaixo no arquivo de zona reverso:

```
1  IN  PTR  pc-1.exemplo.com.br      ; no arquivo de mapeamento reverso
```

Isto significa que ao modificar registros `IN A` no arquivo de mapeamento direto, é necessário efetuar as modificações correspondentes nos registros `IN PTR` do arquivo de configuração de mapeamento reverso.

O ideal seria que existisse apenas um registro e um arquivo tanto para o mapeamento direto quanto para o reverso. Se fosse assim, as situações de erro expostas a seguir não existiriam:

[39] A implementação do serviço de nomes mais utilizada no mundo.

- você pode adicionar um registro A e esquecer do mapeamento reverso, não adicionando o registro PTR correspondente;
    - Em geral, adicionar o registro A (de mapeamento direto) é intuitivo [DNS&BIND], afinal, a função mais famosa do serviço de nomes é mapear nomes em IPs. Por outro lado, adicionar o registro PTR correspondente já não é tão intuitivo assim, podendo ser uma tarefa facilmente esquecida.
- por um descuido, você pode ter registros A e PTR que não casam;
    - Como o mapeamento reverso é muitas vezes esquecido, após atualizações em registros A você pode esquecer de corrigir também o registro `PTR` correspondente, e acabar causando um descasamento entre estes registros.
- situações inversas – apesar de muito mais raras – também podem ocorrer: esquecer de adicionar o registro `IN A` ou esquecer de modificá-lo após inserir ou alterar um registro `IN PTR`.

Este descasamento de registros `A` e `PTR` – seja pela inexistência de um deles, seja por erro de configuração – poderá causar problemas de autenticação à máquina envolvida no descasamento [DNS&BIND]. Suponha, por exemplo que os registros da máquina pc-1 apresentados acima estivessem descasados, ou que o registro PTR não existisse. Então, o usuário de pc-1 poderia ser prejudicado.

Muitos serviços de rede, como por exemplo `FTP`, `ssh`, `telnet` e `rsh`, podem ser compilados ou configurados para agir de forma muito segura (modo paranóico):

ao receber uma requisição de abertura de conexão de um cliente, o servidor recupera o IP cliente e tenta descobrir qual o nome correspondente a este IP (mapeamento reverso);

se o mapeamento reverso tiver sido realizado com êxito, o servidor tenta descobrir o IP correspondente ao nome que acabou de ser descoberto (mapeamento direto);

se o mapeamento direto levar ao mesmo IP do cliente que solicitou a abertura de conexão com o servidor, esta será aceita;

se o mapeamento direto levar a outro IP a conexão será negada;

se o mapeamento reverso não for possível o servidor não aceitará a conexão solicitada.

Alguns servidores podem ser configurados/compilados de forma menos rígida e mesmo que o mapeamento reverso não seja possível (passo b), a conexão será estabelecida. No entanto, o cliente terá que esperar um certo tempo antes de ver que sua conexão foi aceita.

Portanto, quando os registros `A` e `PTR` que definem IP/nome de uma determinada máquina estão descasados ou um dos dois não existe, alguns

serviços podem não funcionar para usuários que usam esta máquina, ou ainda o usuário terá que esperar um algum tempo pelo estabelecimento das conexões com os servidores.

A correspondência correta entre registros `A` e `PTR` deve existir sempre, em qualquer que seja a implementação DNS utilizada. Alguns servidores DNS podem dar uma mãozinha e lhe lembrar do registro `PTR`. No gerenciador do servidor DNS do Windows 2000, por exemplo, a tela para inserir ou modificar registros de endereço oferece a opção de ter o registro `PTR` correspondente criado ou modificado automaticamente.

7.2.2 Sintomas

O usuário da máquina envolvida no erro de configuração de DNS reclamará que alguns serviços não funcionam. No exemplo da seção anterior, o usuário de pc-1 poderia reclamar que não consegue usar `telnet`, `FTP` ou `ssh` para alguns destinos. Neste caso a reclamação pode ser também que precisam esperar algum tempo quando vão se conectar a certos servidores.

7.2.3 Sinais

Procedimento

12.5

Resolução direta de um nome de máquina não casa com a resolução reversa no servidor de nomes primário do domínio. Este sinal será percebido em duas situações:

- os registros `IN A` e `IN PTR` existem, mas não são compatíveis entre si. Por exemplo, no arquivo de configuração do mapeamento direto o endereço IP de pc-1.exemplo.com.br é 192.168.1.1, mas no arquivo de mapeamento reverso o endereço 192.168.1.1 aponta para a máquina pc1.exemplo.com.br;

- um dos registros não existe, tornando o mapeamento direto possível enquanto o reverso não existe ou vice-versa.

7.2.4 Testes confirmatórios

O sinal apresentado na seção anterior é diferencial. Portanto, se ele for encontrado a existência do problema está confirmada.

7.2.5 Sugestões de tratamento

Se o problema foi confirmado corrija o arquivo de configuração adequado. Lembre-se de aumentar o número de série do arquivo modificado. Em seguida reinicialize o servidor DNS.

No servidor DNS BIND, corrija os arquivos necessários com o editor de texto de sua preferência. Incremente o número de série dos arquivos modificados e reinicie o servidor. Você pode reiniciar o `named` de diversas formas. Em versões 9.x o comando `rndc` pode ser utilizado. No BIND 8.x o comando

correspondente ao rndc é o ndc. No entanto, o BIND deve estar devidamente configurado para ser controlado por eles.

```
# rndc reload
# ndc reload
```

Em todas as versões:

```
# kill –HUP <número do processo named>
```

O número do processo named pode ser encontrado com um dos seguintes comandos:

ps –ae | grep named (em sistemas baseados no BSD),

ps –ef | grep named (sistemas baseados no System V)

cat /var/run/named.pid

É possível que com o comando ps você encontre vários processos named em execução. Envie o sinal –HUP apenas para o processo pai (o processo named com menor *pid*).

No servidor DNS do Windows 2000 entre no gerenciador do DNS (Iniciar > Programas > Ferramentas Administrativas > DNS) e modifique os registros apropriados para corrigir o descasamento.

7.3 Inconsistência entre registros dos servidores DNS primário e secundários

7.3.1 Descrição

Leia mais sobre DNS no apêndice 10

Cada arquivo de configuração de nomes tem um número de série associado a ele. Este número de série é utilizado para manter a consistência dos dados armazenados pelo servidor de nomes primário e secundários. Ao modificar um arquivo de configuração de nomes no servidor de nomes primário, o número de série associado a este arquivo deve ser aumentado. Os servidores escravos (secundários) comparam o número de série dos arquivos que estão no servidor principal com os números de série correspondentes em seus arquivos. Se o número de série do servidor principal for maior que o número de série dos arquivos locais, os servidores escravos fazem a transferência da zona com número de série maior, pois neste caso, o arquivo novas configurações foram feitas.

Nas versões do BIND[40] anteriores à 8, o comportamento padrão do servidor secundário é o seguinte: após a inicialização e sempre que se passar um intervalo de tempo igual ao tempo de *refresh* configurado no SOA, o servidor secundário busca os números de série dos arquivos do servidor principal. Quando o

[40] Uma das implementações do serviço de nomes mais usadas no mundo atualmente.

número de série de uma zona do servidor primário for maior que o do servidor secundário, as informações desta zona serão transferidas para o servidor secundário, garantindo a consistência dos dados dos servidores.

Nas versões mais novas do BIND (8 e 9), o servidor de nomes primário envia para os servidores escravos mensagens de notificação sempre que é reinicializado. Ao receber uma mensagem de notificação, os servidores secundários agem como se o tempo de *refresh* tivesse expirado: comparam os números de série e efetuam a transferência das zonas cujos números de série cresceram. Assim, o servidores secundários não precisam esperar que o intervalo de *refresh* passe para que eles busquem modificações nos arquivos de configuração de nomes do servidor principal.

O fato é que, em qualquer versão do BIND, informações só são copiadas do servidor primário para os secundários quando estes verificam que o número de série do arquivo no servidor primário é maior.

Desta forma, se você modificar um arquivo de configuração de nomes do servidor primário e esquecer de aumentar seu número de série, os servidores secundários não considerarão as modificações feitas. Como o número de série não aumentou, os servidores secundários acham que estão com informações atualizadas. Quando os servidores de nomes secundários forem consultados, eles poderão oferecer respostas erradas, causando diversos efeitos colaterais.

Os efeitos dessa inconsistência dependem do tipo de modificação feita e do servidor envolvido. Por exemplo, se a modificação era apenas a troca do endereço IP de uma certa máquina cliente local no servidor de nomes interno, as conseqüências não serão drásticas. O usuário desta máquina pode, por exemplo, não conseguir acessar alguns serviços. Já se o endereço IP do servidor Web da organização foi modificado no servidor de nomes externo, as conseqüências serão mais desastrosas: quando o servidor secundário for consultado, o antigo IP do servidor Web será oferecido, e o *site* de sua empresa não será visto, pois ele estará em outra máquina.

Outro caso em que as conseqüências são de maiores proporções ocorre quando informações sobre um novo sub-domínio são inseridas ou modificadas. O servidor secundário nada saberá!

Uma última observação: os servidores de nomes secundários anteriores à versão 8, como citado anteriormente, só procuram novas versões dos arquivos de configuração do servidor primário de tempos em tempos. Portanto, durante algum tempo, os servidores de nomes escravos podem realmente ficar desatualizados, apesar do número de série ter sido incrementado. Assim, se você está utilizando versões antigas do BIND ou configuradas para não notificar os servidores escravos de modificações nos números de série[41], não queira que os servidores escravos estejam atualizados tão logo você modifique os arquivos do

[41] Diretiva `notify no` arquivo /etc/named.conf. Mais informações em [DNS&BIND].

servidor primário. Eles só estarão atualizados após um ou mais intervalos de *refresh*[42].

7.3.2 Sintomas

Como já mencionado anteriormente, os sintomas percebidos pelos usuários dependem do tipo de modificação que foi realizada e em que servidor. Em geral, a reclamação será de indisponibilidade de alguns serviços.

Se o esquecimento ocorrer quando os dados do servidor de nomes públicos da organização tiverem sido atualizados, pessoas de fora da organização poderão também reclamar que alguns serviços não estão funcionando.

Quando se trata de navegação na Internet o próprio navegador dá dicas de que algo está errado com o DNS. Quando não for possível resolver o nome do servidor, ou quando o IP resultante da resolução for incorreto, o navegador passará algum tempo localizando a máquina ou tentando abrir a página. No Internet Explorer, por exemplo, após esse tempo, uma página de erro é apresentada, contendo mensagens como: "`Não é possível encontrar <nome-da-maquina>`" ou "`A página não pode ser exibida (…) Não é possível encontrar o servidor ou ocorreu um erro de DNS`".

7.3.3 Sinais

Procedimento **12.1**

Os servidores primário e secundários retornarão respostas diferentes a uma mesma consulta DNS. Os servidores secundários não consideram as modificações de configuração mais recentes. Portanto, ao realizar consultas envolvendo estas modificações, as respostas dos servidores primário e secundários serão incompatíveis.

Procedimento **11.14**

Percebemos que há conectividade através dos endereços IPs das máquinas envolvidas no erro, mas não através de seus nomes de domínio.

7.3.4 Testes confirmatórios

O sinal apresentado na seção anterior é diferencial, portanto, você pode confirmar o problema seguindo os passos do VERIFICANDO CONSISTÊNCIA DE DADOS NOS SERVIDORES DNS PRIMÁRIO e secundários (página 343).

Lembre-se que, se o servidor primário não estiver notificando os escravos ao ser reiniciado, os servidores escravos levarão realmente algum tempo (tipicamente será no máximo o tempo de *refresh*) para perceber a modificação.

---

[42] Um servidor escravo pode ser configurado para atualizar seus dados com base nos dados de outro servidor escravo. Assim, pode ser necessário duas vezes o tempo de *refresh* para ele perceber a modificação.

7.3.5 Sugestões de tratamento

Uma boa prática de configuração é utilizar números de série no seguinte formato [RFC1912]:

```
YYYYMMDDnn
```

Os dígitos YYYY indicam o ano da modificação, MM indicam o mês, DD o dia e nn a quantidade de vezes que o arquivo foi modificado no dia.

Por exemplo, se no dia trinta de janeiro de 2002 você está modificando o arquivo named.zone pela terceira vez, o número de série que você colocaria nele seria: 2002013003.

Você acabou de descobrir que esqueceu de modificar o número de série de um certo arquivo de configuração de nomes. Para solucionar o problema mude o número de série deste arquivo como se ele tivesse sido modificado agora. Se hoje é 29 de janeiro de 2002, mude o número de série do arquivo em questão para 2002012901. Em seguida, reinicialize o servidor de nomes primário como apresentado na página 177.

O servidor DNS do Windows 2000 incrementa o número de série automaticamente quando você modifica alguma configuração de zona usando a interface de gerenciamento do DNS (Iniciar > Programas > Ferramentas Administrativas > DNS). No entanto, ele não seguirá a prática de associar o número de série à data da modificação.

7.4 O TTL *default* de uma zona DNS não está configurado

7.4.1 Descrição

Leia mais sobre DNS no apêndice 10

Antes de entender este problema é preciso entender o que é o TTL (*Time to Live*) *default* de uma zona. Veja o exemplo seguinte:

Considere os servidores de nomes do domínio exemplo.com.br e do domínio cisco.com. Eles serão chamados aqui ns.exemplo.com.br e ns.cisco.com[43]. Quando um usuário do domínio exemplo.com.br deseja visitar a página www.cisco.com, o servidor de nomes ns.exemplo.com.br é consultado: "ns.exemplo.com.br, qual é o endereço IP correspondente ao nome www.cisco.com?". Como ns.exemplo.com.br não sabe resolver este nome localmente e esta resolução também não se encontra em sua *cache*, ele consulta um dos servidores raiz configurado em seu arquivo de dicas.

[43] Na realidade, neste exemplo, sempre que você vir o nome ns seguido do nome do domínio, considere que esta é a máquina servidora de nomes do domínio.

O servidor raiz também não sabe quem é www.cisco.com[44], mas ele sabe quem é o servidor do domínio .com e fornece esta informação para ns.exemplo.com.br, que em seguida, consulta um dos servidores ns.com. Este servidor informa a ns.exemplo.com.br que não sabe quem é www.cisco.com, mas sabe quem é o servidor do domínio cisco.com. Ao consultar ns.cisco.com, o servidor de nomes ns.exemplo.com.br pode obter uma resposta positiva, ou uma resposta negativa.

Em caso de resposta positiva, ns.cisco.com informa para ns.exemplo.com.br o endereço IP de www.cisco.com, e informa também por quanto tempo esta informação pode ser utilizada com segurança por ns.exemplo.com.br. A este tempo dá-se o nome de TTL *default*. O servidor ns.exemplo.com.br irá armazenar esta resolução positiva em uma *cache* durante o tempo correspondente ao TTL *default* fornecido. Durante este tempo, sempre que um cliente do servidor ns.exemplo.com.br consultá-lo para resolver o nome www.cisco.com, o servidor utilizará a informação que está em sua *cache*.

É possível que TTLs sejam configurados para cada registro individualmente. Assim, se o TTL *default* de uma zona é X e o TTL de um registro é Y, este registro será armazenado em outros servidores durante um tempo igual a Y. Neste caso o TTL *default* não é quem dita o tempo de armazenamento do registro na *cache*. O mesmo cuidado que se deve ter com o valor do TTL *default* vale para TTLs de registros individuais.

Pode ocorrer também que a resposta à consulta seja negativa. Este é o segundo caso mencionado acima. ns.cisco.com, por alguma razão, não foi capaz de resolver o nome www.cisco.com, apesar de ser o servidor de nomes deste domínio. As respostas negativas, assim como as positivas, também são armazenadas em uma *cache* durante um tempo chamado TTL de respostas negativas.

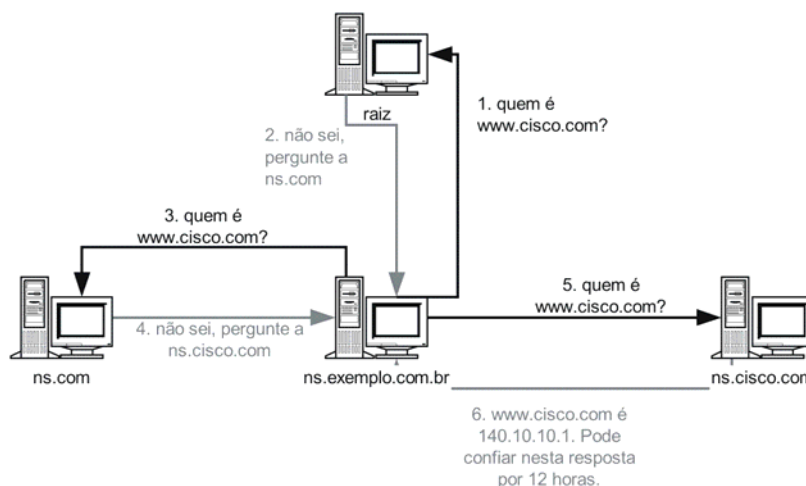



Figura 7-1: Exemplo do funcionamento do serviço de nomes.

[44] Alguns servidores raiz respondem por domínios de genéricos de alto nível (tais como edu, com, gov e mil) [DNS&BIND].

A partir da versão 8.2 do BIND, a forma de configurar o TTL *default* foi modificada [DNS&BIND]. Nas versões anteriores a esta, o TTL *default* era configurado no último campo do registro SOA. No entanto, o significado deste campo foi alterado e ele passou a definir o TTL de respostas negativas. Assim, a partir desta versão, o TTL *default* passou a ser configurado através da diretiva `$TTL`. Se o TTL *default* não estiver devidamente configurado através da diretiva `$TTL` as versões do BIND superiores à versão 8.2 alertarão o problema no arquivo de *logs* e uma das seguintes situações ocorre: o `named` não entra em execução, ou entra em execução mas não resolve os nomes locais, ou ainda funciona normalmente.

Na data da publicação deste livro, a versão mais nova do BIND é a 9.2. Por questões de compatibilidade com as implementações mais antigas, o BIND 9.2 funcionará mesmo sem a diretiva `$TTL`. O último campo do registro `SOA` – como antigamente – será utilizado para definir o TTL *default*. Mas o BIND 9.2 irá indicar o erro em seu arquivo de *logs* e o `named-checkzone` também alertará sobre o problema.

Em resumo, se 1) você utiliza a implementação BIND do DNS, 2) a versão em operação está entre 8.2 (inclusive) e 9.2 e 3) você esqueceu de configurar o TTL *default* de uma zona com a diretiva `$TTL`, o seu servidor de nomes poderá não resolver nomes locais ou simplesmente não ser executado. Se você utiliza outras versões do BIND ou outras implementações do DNS não se preocupe com este problema. Este é um problema intimamente relacionado à implementação BIND. No servidor DNS do Windows 2000 o TTL *default* ainda é configurado no registro SOA, no campo *minimum TTL*.

É mais provável que este problema ocorra quando você estiver migrando de uma versão do BIND mais antiga para uma mais nova.

7.4.2 Sintomas

Em muitas organizações tem-se um servidor de nomes interno, responsável pela resolução dos nomes locais, e um servidor de nomes externo, que responde pelos nomes de domínio público da organização.

Quando o servidor de nomes interno estiver sem a configuração do TTL *default*, os usuários reclamarão que:

não conseguem acessar os serviços locais, mas conseguem acessar a Internet. No entanto, como não há resolução de nomes locais, alguns serviços como telnet, ssh e FTP podem não funcionar, mesmo quando o servidor não for uma máquina local. Quando um cliente FTP, por exemplo, tenta conectar-se ao servidor FTP, este tenta a resolução reversa de nomes a partir do IP do cliente[45]. Sem a resposta do servidor de nomes, por questões de segurança, a conexão não será estabelecida. É o mesmo que ocorre quando os registros `A` e `PTR` não casam (problema apresentado na página 175).

---

[45] Nem todos os servidores têm este mesmo comportamento, só os que são compilados ou configurados para agir assim – modo paranóico.

a rede não está funcionando. Ao tentar navegar na Internet, por exemplo, o próprio navegador apresentará uma página de erro indicando erro de DNS.

Quando o servidor de nomes externo está com este problema, pessoas que não estão na organização podem reclamar. Elas dirão que os serviços oferecidos pela sua organização não estão funcionando. Por exemplo, não estão conseguindo navegar no *site*, efetuar transferência de arquivos nem enviar/receber *e-mails* de usuários internos. O próprio navegador informa o erro de DNS.

7.4.3 Sinais

Procedimento
12.2

Quando a diretiva $TTL não está presente no arquivo de configuração, o BIND alerta o gerente com uma mensagem no arquivo de *log*. No BIND 9.2, por exemplo, a mensagem é "No default TTL set using SOA minimum instead". Será indicado no arquivo de *log* também o arquivo onde o TTL *default* não está configurado.

7.4.4 Testes confirmatórios

O sinal apresentado na seção anterior é confirmatório. Se ele foi encontrado nenhum teste adicional precisa ser realizado.

7.4.5 Sugestões de tratamento

A diretiva $TTL deve ser inserida no arquivo de configuração onde o TTL *default* não foi configurado antes do registro SOA. Todos os arquivos de configurações de nomes (mapeamento direto, reverso e local) devem ter a diretiva $TTL. Veja o exemplo a seguir:

```
$TTL 86400
@       IN      SOA     ns.exemplo.com.br. root.exemplo.com.br. (
                                200201231       ; Serial
                                8h              ; Refresh – 8 Horas
                                2h              ; Retry – 2 Horas
                                2w              ; Expire – 2 Semanas
                                2h)             ; Minimum TTL – 2 Horas
```

Nos arquivos de configuração de zonas do BIND tudo que vem após um ponto e vírgula (;) é considerado comentário. Neste exemplo, o TTL default é 86400 segundos, que equivale a 1 dia. Ao TTL de respostas negativas foi atribuído o valor de 2 horas. O TTL default deve ser escolhido de acordo com a freqüência de mudanças em mapeamentos nome ↔ IP em sua rede. Para uma melhor sintonização do seu servidor DNS leia o problema **TTL E OUTROS CAMPOS DO REGISTRO SOA COM VALORES INADEQUADOS**.

Ao inserir a diretiva $TTL nos arquivos de zonas onde ela não existia lembre-se de reiniciar o servidor DNS:

```
# kill –HUP <número do processo named>
```
[46]

Para evitar este problema (e outros problemas com BIND), sempre que modificar algum dos arquivos de configuração de nomes ou que atualizar a versão do BIND para uma mais nova, verifique a sintaxe dos arquivos de configuração de nomes. Esta verificação pode ser realizada com a ferramenta `named-checkzone`, que é instalada com o `named`. A sintaxe de utilização desta ferramenta é[47]:

```
# named-checkzone <nome do arquivo a ser verificado>
```

Por exemplo, considere que o arquivo /var/named/named.zone contém configurações de nomes locais do domínio exemplo.com.br. Então, para verificar se este arquivo está correto execute[48]:

```
# named-checkzone /var/named/named.zone
```

Esta ferramenta também pode (e deve!) ser utilizada para verificar os demais arquivos de configuração de nomes do servidor (reverso e local). Caso a diretiva `$TTL` não exista em um destes arquivos de configuração, o `named-checkzone` informará claramente.

7.5 DNS: TTL e outros campos do registro SOA com valores inadequados

7.5.1 Descrição

Leia mais sobre DNS no apêndice 10

No problema **O TTL DEFAULT DE UMA ZONA DNS NÃO ESTÁ CONFIGURADO** (página 181) o significado do TTL (*Time to Live*) *default* já foi apresentado. Em resumo, quando um cliente solicita a um servidor DNS que resolva um nome não local, o servidor irá iniciar a busca a partir de um servidor de nomes raiz[49]. Até que o nome seja resolvido, outros servidores serão consultados. Finalmente, o servidor responsável pelo domínio a que o nome em questão pertence é consultado e o nome é resolvido. Além de informar o mapeamento nome → IP (ou IP → nome), o servidor deste domínio informa também por quanto tempo este mapeamento é válido. Este tempo é chamado TTL *default*[50]. O servidor que

---

[46] Este número pode ser obtido com o comando `# ps –ae | grep named`.

[47] No BIND 9.2 o aplicativo `named-checkzone` precisa ainda receber o nome do domínio a ser checado. O comando então é:
```
# named-checkzone <domínio> <arquivo a ser verificado>
```

[48] No BIND 9.2 o comando seria: `# named-checkzone exemplo.com /var/named/named.zone`

[49] Na realidade isto ocorrerá apenas se a resolução solicitada não estiver armazenada na *cache* do servidor.

[50] É possível que TTLs sejam configurados para cada registro individualmente. Assim, pode ser que o tempo de armazenamento de um registro em outro servidor não seja o TTL *default* e sim o TTL configurado para o registro individualmente.

recebe a resposta armazena-a em uma *cache* local durante um intervalo de tempo igual ao TTL recebido.

Durante este tempo, se outros clientes solicitarem a resolução do mesmo nome, o servidor não mais precisará buscá-lo externamente, ele utilizará os dados da *cache*. É como se um servidor de nomes, ao responder uma consulta a outro servidor de nomes, dissesse: "amigo, confie nesta resposta por x segundos. Por favor, durante este tempo não venha me fazer esta mesma pergunta novamente!".

Além do TTL *default* existem outros valores de tempo que devem ser definidos no registro SOA. Dentre eles encontram-se[51]: intervalo de *refresh* e o TTL de respostas negativas. Quando algum destes campos está com um valor inadequado, você pode enfrentar alguns problemas com o serviço DNS. Antes de continuar, veja o que cada um destes campos significa:

- *Refresh* → de quanto em quanto tempo o servidor secundário verifica se o número de série do servidor primário foi alterado (caso em que o secundário faz uma nova transferência de zona);

- TTL de respostas negativas → se um servidor de nomes não for capaz de resolver o nome (ou o IP) de uma máquina do seu domínio, a resposta negativa também será armazenada em uma *cache*. O TTL de respostas negativas indica por quanto tempo a resposta negativa oferecida por este servidor de nomes deve ser armazenada na *cache* de outros servidores DNS. Apenas servidores DNS mais novos são capazes de armazenar respostas negativas.

Ao escolher o TTL para seus dados você deve, na realidade, optar entre desempenho e consistência [DNS&BIND]. Um TTL bem pequeno vai assegurar que outros servidores não armazenarão em *cache* dados sobre seu domínio por muito tempo, e serão obrigados a consultá-lo, garantindo que mudanças logo serão percebidas por todos. Por outro lado, isto aumenta o número de pesquisas realizadas nos servidores de nomes de sua organização, podendo sobrecarregá-los, tornando a resolução de nomes mais lenta. Já com um TTL maior, os seus servidores de nomes não ficarão tão sobrecarregados. No entanto, os dados sobre os nomes de seu domínio armazenados em outros servidores podem ficar inconsistentes por um longo tempo. Isto se deve ao fato de que outros servidores de nomes armazenarão informações sobre nomes do seu domínio por mais tempo. Neste caso, o problema mais grave é percebido quando são realizadas modificações em registros que definem nome → endereço de servidores. O serviço pode ficar indisponível por um longo período – um período inaceitável.

Em resumo, TTLs muito grandes podem gerar inconsistência de dados, resultando em mapeamentos incorretos e interrupção de serviços. Quando o TTL é muito pequeno o que pode ocorrer é uma quantidade muito grande de requisições de resoluções de nomes aos servidores DNS de sua organização, podendo seu desempenho ficar prejudicado.

[51] Existem ainda outros campos que serão citados apenas na seção **SUGESTÕES DE TRATAMENTO**.

Um intervalo de *refresh* muito grande também pode causar inconsistência de dados entre o servidor primário e os secundários. Se o servidor primário estiver configurado para notificar os secundários sobre mudanças em arquivos de zonas[52] não há problema. Mas, quando o servidor primário não oferece esta funcionalidade ou não está configurado para tal, os servidores secundários podem passar bastante tempo armazenando informações inconsistentes. Imagine um *site* com mudanças diárias em arquivos de zonas. Se o intervalo de *refresh* for 2 dias e o servidor primário não estiver configurado (ou capacitado) para notificar os secundários sobre mudanças, os servidores secundários podem ficar desatualizados por até 2 dias. O resultado é o mesmo que ocorre quando você muda um arquivo de uma zona e esquece de incrementar o seu número de série (ver problema **INCONSISTÊNCIA ENTRE REGISTROS DOS SERVIDORES DNS PRIMÁRIO E SECUNDÁRIOS**). Os servidores DNS secundários oferecerão respostas erradas aos clientes.

Se o TTL de respostas negativas for muito grande – maior que um dia, por exemplo – as respostas negativas oferecidas pelo seu servidor DNS podem ficar armazenadas em outros servidores de nomes por muito tempo, podendo deixar alguns serviços sem funcionar.

Note que quando o valor do TTL *default* ou intervalo de *refresh* está muito grande, os problemas só ocorrerão quando algum registro for modificado, em especial, um registro que defina o mapeamento nome → endereço IP de um servidor. Já quando estes valores são muito pequenos, o problema pode ser percebido independente de modificações terem sido realizadas. Quanto mais sobrecarregado estiver o servidor, mais perceptível será o sintoma. Em se tratando de servidores pouco consultados, o problema de desempenho pode nem ser percebido.

7.5.2 Sintomas

Se o servidor DNS do domínio público estiver com TTL *default* ou TTL de respostas negativas muito grande e modificações em registros de servidores forem realizadas, usuários de outros domínios podem não conseguir acessar alguns serviços. Lembre-se: este sintoma será percebido apenas quando alterações que envolvem nomes/endereços de servidores forem realizadas no servidor DNS. Se você mudou o IP do servidor Web, SMTP ou FTP, por exemplo, usuários externos e internos podem não conseguir navegar nas páginas Web do seu *site*, enviar mensagens para seus usuários ou fazer transferência de arquivos durante um bom tempo.

Se o TTL *default* estiver muito pequeno muitas requisições de resoluções de nomes chegarão ao servidor DNS. O servidor de nomes pode ficar sobrecarregado, ou ainda enlaces de menor capacidade podem ficar saturados. Os usuários internos e/ou externos podem reclamar de lentidão na rede ou no

[52] Nas versões 8.2.3 e superiores do BIND, por *default*, servidores primários enviam mensagens de notificação aos servidores secundários de uma zona quando ela é modificada. Os servidores BIND v8 anteriores à versão mencionada anteriormente precisam ser explicitamente configurados para tal (opção `notify yes`). Versões anteriores à 8 não suportam a notificação [DNS&BIND].

acesso aos serviços. Na realidade a lentidão pode estar sendo causada pela sobrecarga dos servidores de nomes ou pela saturação de enlaces. Se o intervalo de *refresh* está muito pequeno os servidores secundários irão realizar pesquisas SOA no servidor primário muitas vezes, podendo aumentar ainda mais carga de requisições e a utilização de enlaces. No entanto, se apenas o intervalo de *refresh* está muito pequeno, é mais provável que a sobrecarga não seja observada. Suponha que o intervalo de *refresh* de uma zona é 5 minutos e existem 2 servidores secundários. A cada 5 minutos pelo menos 2 pesquisas SOA serão realizadas no servidor primário.

Quando o tempo de *refresh* está muito grande e modificações em registros de servidores são realizadas, os servidores DNS secundários poderão ficar desatualizados por algum tempo, oferecendo respostas erradas e deixando alguns serviços indisponíveis.

7.5.3 Sinais

Procedimento **10.6**

Se o TTL *default* estiver muito pequeno e o número de requisições ao servidor de nomes for muito grande, é possível que o servidor DNS apresente uma utilização elevada de CPU. O limiar de advertência para utilização de CPU é 75%.

Procedimento **10.10**

Se o TTL *default* estiver muito pequeno, o número de requisições ao servidor de nomes for muito alta e existirem enlaces de pequena capacidade entre o servidor sobrecarregado e os seus clientes, é provável que estes enlaces fiquem saturados antes mesmo que o servidor fique sobrecarregado. Nestas circunstâncias, é possível encontrar enlaces de menor capacidade (longa distância, em geral) saturados devido ao tráfego DNS. O limiar para utilização de enlaces de acesso não compartilhado é 70%.

Procedimento **12.1**

Quando o intervalo de *refresh* for muito grande os servidores primário e secundários poderão retornar respostas diferentes a uma mesma consulta DNS durante algum tempo. Isto também ocorrerá se você modificar algum arquivo no servidor primário e esquecer de incrementar o número de série associado ao arquivo.

7.5.4 Testes confirmatórios

RESUMO DOS TESTES

Se o sintoma é rede lenta:

TESTE 1

Verifique o valor do TTL *default* e do intervalo de *refresh* nos arquivos de zonas dos servidores DNS primários;

Se o sintoma é indisponibilidade de serviços:

TESTE 2

Modificações em registros do servidor primário foram realizadas? Verifique o TTL *default* e os valores do SOA configurados.

Teste confirmatório 1

Infelizmente, não existem testes específicos – aplicativos a serem utilizados, por exemplo – que definam com clareza quando o TTL *default* ou qualquer outro valor do registro SOA estão muito pequenos.

Se você está observando utilização alta de CPU nos servidores DNS de uma zona verifique que processo está consumindo mais CPU. Se o maior consumidor de CPU for o servidor de nomes ou enlaces de longa distância estiverem saturados, verifique o valor do TTL *default* e do tempo de *refresh* no servidor primário.

O TTL *default*, geralmente, varia entre algumas horas e alguns dias (menos que uma semana). Se você observar um valor bem menor que uma hora, por exemplo, desconfie que esta é a causa do problema. Aumente o valor do TTL *default* e verifique também os valores do SOA alterando-os para um valor mais adequado, se necessário. Se com esta alteração os sintomas e sinais cessaram o problema foi confirmado.

Se o valor do TTL *default* está adequado – 12 horas, por exemplo – a causa da lentidão na rede é outra.

Teste confirmatório 2

Se após modificar um registro que define o nome ou o endereço de um servidor foi observada indisponibilidade do serviço oferecido por ele, o problema está praticamente confirmado. Verifique o valor do TTL *default* da zona a que o servidor pertence no servidor de nomes primário desta zona. Se ele estiver muito grande – uma semana, por exemplo – o problema foi confirmado.

Na realidade, sempre que modificações em registros de servidores forem realizadas alguns cuidados devem ser tomados (ver Seção **SUGESTÕES DE TRATAMENTO**). Caso contrário, o serviço oferecido pelo servidor cujo nome/IP foi modificado ficará indisponível durante um certo tempo, no máximo igual ao TTL *default* ou ao TTL explícito do registro modificado.

7.5.5 Sugestões de tratamento

Existem outros valores do registro SOA além dos citados anteriormente que não devem ser esquecidos. A seguir é dada uma breve descrição de cada um deles:

- *Retry* → se o servidor secundário não conseguir falar com o servidor primário após o intervalo de *refresh*, de quanto em quanto tempo ele ficará tentando falar com o servidor primário para verificar se precisa ou não ser atualizado;

- Expiração → quando o servidor secundário não consegue falar com o primário, por quanto tempo ele ainda considerará válidas suas informações e continuará oferecendo a clientes respostas relacionadas ao domínio.

Como citado anteriormente, você deve fazer uma escolha entre desempenho e consistência. Mas, em [RFC1912, RFC2308, DNS&BIND] alguns valores típicos são recomendados para o TTL *default* e demais campos do registro SOA:

- TTL *default* → valores típicos variam algumas horas e 5 dias. No entanto, você deve escolher um valor condizente com a quantidade de atualizações feitas no servidor de nomes. Valores maiores que 1 dia são menos freqüentes. Na dúvida, escolha um TTL *default* de 12 horas ou 1 dia;

- *Refresh* → você pode escolher um tempo pequeno (20 minutos a 2 horas) se você não tem preocupação com um aumento de pesquisas no servidor primário e da utilização dos enlaces. Pode escolher um valor maior, quando conexões mais lentas e de longa distância são utilizadas. Não é recomendado que se use um valor maior que 1 dia;

- *Retry* → geralmente é uma fração do tempo de *refresh*. Se o tempo de *refresh* for 2 horas, por exemplo, o tempo de *retry* pode ser 30 minutos.

- *Expire* → 1 a 4 semanas são os valores sugeridos. Este valor deve ser maior que o maior tempo possível de duração de uma falha em sua rede. Ele deve ser maior que o tempo de *refresh*, para evitar que os dados do servidor secundário expirem antes dele ter a oportunidade de fazer uma nova cópia;

- TTL de respostas negativas → valores entre 1 e 3 horas têm se mostrado razoáveis. Valores maiores que 1 dia são problemáticos.

Se você usa a implementação BIND do serviço DNS, modifique o registro SOA e a diretiva TTL dos arquivos de configurações de zonas. Configure neles valores mais adequados. Abaixo seguem valores típicos:

```
$TTL 86400    ; 86400 Segundos (1 dia)4
@       IN      SOA    ns.exemplo.com.br. root.exemplo.com.br. (
                                200201231      ; Serial
                                4h             ; Refresh – 4 Horas
```

```
1h          ; Retry – 1 Hora
2w          ; Expire – 2 Semanas
2h)         ; TTL neg. – 2 Horas
```

Para modificar valores do registro SOA no Windows 2000 escolha Iniciar > Programas > Ferramentas Administrativas > DNS. Expanda o servidor de nomes e clique com o botão direito do mouse sobre a zona cujo SOA você deseja modificar. Escolha o item Propriedades. Escolha a tabela Start of Authority (SOA) e modifique os valores configurados para corrigir o problema.

Ao modificar o TTL *default* e outros valores do registro SOA lembre-se de reiniciar o servidor DNS. No Linux isto pode ser feito com o comando `kill`:

```
# kill –HUP <número do processo named>
```

Em geral, modificações em registros que envolvem máquinas clientes são bem mais freqüentes. O problema grave ocorre quando são realizadas modificações em registros que envolvem servidores, por exemplo, mudar o endereço IP do servidor Web da empresa. Se o TTL for grande, outros servidores DNS podem utilizar o mapeamento nome ⇨ endereço antigo armazenados em *cache* por muito tempo, impossibilitando aos clientes o acesso ao serviço Web.

Para resolver este problema lembre-se que os valores do TTL *default* e de TTLs explícitos não são imutáveis. Você pode escolher um valor adequado, mas pode modificá-lo quando necessário. A seguir vai uma dica do que fazer para não sofrer indisponibilidade de serviços ao modificar algum registro que envolva definição de endereços de servidores: algum tempo antes de realizar a modificação do IP do servidor diminua o TTL *default* ou o TTL explícito dos registros que serão modificados. Com isso, garante-se que outros servidores DNS irão armazenar dados sobre seu domínio na *cache* por menos tempo, e perceberão mais rapidamente as mudanças que ocorrerem. Alterar o TTL imediatamente antes de realizar a troca de IP não vale. Você tem que diminuir o TTL com mais antecedência. Pelo menos com uma antecedência igual à soma do intervalo de *refresh* e do TTL utilizados. Este tempo é necessário para que os dados de seu domínio armazenados na *cache* de outros servidores DNS expirem e eles consultem o seu servidor novamente. Os resultados das novas consultas já informação um TTL menor. Além disso, os servidores secundários também serão atualizados e passarão a fornecer um TTL pequeno.

Suponha que você precise mudar o endereço IP do servidor Web. Se seu TTL *default* é 1 dia e o intervalo de *refresh* é 2 horas, você deve diminuir o TTL *default* ou o TTL explícito dos registros de nomes do servidor Web pelo menos 26 horas antes de realizar a troca do IP no servidor Web. Diminua o TTL *default* para o tempo máximo durante o qual o serviço em questão pode ficar indisponível. Altere o TTL para 30 minutos, por exemplo. Assim, ao alterar o IP do servidor Web o serviço será interrompido por no máximo 30 minutos.

7.6 Falta “.” após nomes totalmente qualificados em registros DNS

7.6.1 Descrição

Leia mais sobre DNS no apêndice 10

Todos os nodos na árvore de nomes de domínio podem ser identificados por um FQDN. Esta é a abreviação de *Fully Qualified Domain Name* (nome de domínio totalmente qualificado). O nome mail.exemplo.com.br, por exemplo, é um nome de máquina totalmente qualificado. Ele indica o caminho que deve ser percorrido desde a raiz da árvore de nomes de domínio até se chegar a ele. Nomes não totalmente qualificados são nomes relativos a algum nodo da árvore de nomes de domínio inferior à raiz. Por exemplo, o nome de máquina mail. Este nome não é interpretado com relação à raiz, como os FQDNs, mas sim em relação a algum sub-domínio inferior a ela. Neste exemplo, este nome é interpretado com relação ao nodo exemplo.com.br.

Nos arquivos de zonas DNS os nomes de máquinas podem estar escritos em sua forma completa (FQDNs) ou não. Quando um nome termina com um “.” (ponto) o servidor considera que ele é um FQDN. Caso contrário o servidor DNS interpreta-o como sendo relativo à zona sendo configurada. Neste caso o nome da zona é adicionado automaticamente após o nome configurado no arquivo.

Suponha que você está configurando o mapeamento direto do domínio exemplo.com.br. Você deseja configurar o nome de um servidor Web, que é www.exemplo.com.br. Uma das seguintes linhas deve ser inserida no seu arquivo de zonas:

```
www                           IN      A              200.120.10.100
```

ou

```
www.exemplo.com.br.    IN      A              200.120.10.100
```

O nome www encontrado na primeira linha será interpretado pelo servidor DNS como um nome relativo ao domínio exemplo.com.br. Suponha que você resolveu utilizar em seus arquivos de zonas nomes completamente qualificados (a segunda linha descrita no exemplo anterior). No entanto, você esqueceu de colocar o “.” No final do nome de uma máquina. A linha resultante foi:

```
www.exemplo.com.br     IN      A              200.120.10.100
```

Devido a este erro, o servidor de nomes nada saberá sobre a máquina www.exemplo.com.br. Para ele, www.exemplo.com.br.exemplo.com.br é o nome da máquina cujo endereço IP é 200.120.10.100. Como conseqüência não será possível estabelecer uma conexão com o servidor Web através de seu nome.

Quando o ponto é esquecido na definição de nomes totalmente qualificados de servidores o problema é mais grave, pois os servidores envolvidos não poderão ser acessados pelo seu nome. Se o ponto for esquecido após o nome do

servidor SMTP indicado em um registro MX, por exemplo, você poderá ter problemas com o serviço de Correio Eletrônico.

Um outro problema mais sério ocorre quando o ponto é esquecido na definição de sub-domínios. Nenhum nome do sub-domínio envolvido no erro de configuração poderá ser resolvido. Considere novamente o arquivo de configuração do domínio exemplo.com.br. O que acontece se o sub-domínio gerencia.exemplo.com.br for configurado da seguinte forma:

```
gerencia.exemplo.com.br          IN  NS  server.gerencia.exemplo.com.br.
server.gerencia.exemplo.com.br.  IN  A      200.120.11.53
```

O servidor DNS do domínio exemplo.com.br pode ser consultado a respeito de um nome do sub-domínio gerencia. No entanto, no exemplo acima o servidor DNS nada sabe sobre o sub-domínio gerencia.exemplo.com.br. O sub-domínio que ele conhece é o gerencia.exemplo.com.br.exemplo.com.br. Neste caso, o mundo não saberá como resolver nomes deste sub-domínio. Se o ponto tivesse sido esquecido ao definir quem é o servidor de nomes do sub-domínio, como abaixo, o servidor DNS reconheceria o sub-domínio, mas não saberia informar o endereço IP do servidor DNS responsável por ele.

```
gerencia.exemplo.com.br.        IN   NS    server.gerencia.exemplo.com.br
server.gerencia.exemplo.com.br. IN   A     200.120.11.53
```

Quando os nomes envolvidos identificam máquinas clientes, os usuários destas máquinas podem não conseguir acessar certos serviços (ver problema **DNS: DESCASAMENTO DE REGISTROS A E PTR EM ARQUIVOS DE ZONAS**).

O ponto pode ser esquecido em quaisquer registros dos arquivos de zonas. Sempre que você escrever um FQDN e esquecer do ponto final, estará inserindo erros de configuração em seu servidor DNS, pois ele estará interpretando os dados de forma incorreta.

7.6.2 Sintomas

A reclamação geral será indisponibilidade de serviços. Como já citado, quando o ponto for esquecido após um nome de servidor ou de um sub-domínio, o problema fica mais grave. Esquecer o ponto ao definir nomes e endereços de máquinas clientes nos arquivos levará aos mesmos sintomas apresentados no problema da página 175: o usuário da máquina envolvida reclamará que alguns serviços não estão funcionando ou que precisam esperar algum tempo antes de ter conectividade com os servidores.

Usuários de fora da organização também podem reclamar quando o erro existir na configuração de zonas públicas. Eles podem não conseguir acessar as páginas *Web* de seu *site* ou não conseguir enviar mensagens para usuários de sua organização.

7.6.3 Sinais

Procedimento

12.6

Os sinais apresentados dependem de onde o ponto foi esquecido. Quando se esquece o ponto no fim de um FQDN em um registro IN A, o resultado será que alguns nomes locais só podem ser resolvidos quando de acrescenta o nome do domínio duas vezes. Considerando o exemplo dado na Seção **DESCRIÇÃO**, o nome www poderá ser resolvido quando se pergunta ao servidor quem é www.exemplo.com.br.exemplo.com.br, mas não quando se pergunta quem é www.exemplo.com.br. Se, por exemplo, o ponto foi esquecido em um registro IN PTR, o mapeamento reverso vai levar a um nome de máquina com o nome do domínio mais domínio in-addr.arpa. Por exemplo, o mapeamento reverso de 200.120.10.100 levará a www.exemplo.com.br.10.120.200.in-addr.arpa. Respostas incorretas também será oferecidas quando o ponto for esquecido em registros MX e NS.

7.6.4 Testes confirmatórios

O sinal apresentado na seção anterior é diferencial. Isto significa que se ele for encontrado o problema está confirmado.

7.6.5 Sugestões de tratamento

A solução para este erro é bastante simples e clara: acrescente o ponto onde ele foi esquecido ou passe a utilizar nomes relativos ao domínio (exceto no arquivo dede mapeamento reverso). A segunda opção é bem mais interessante: além de não correr o risco de esquecer o ponto, você precisará escrever menos e poderá mudar o nome do domínio sem precisar modificar muitas configurações no servidor de nomes. Não esqueça de modificar o número de série do arquivo modificado e de reinicializar o serviço de nomes para que as novas configurações tenham efeito.

Nos arquivos de mapeamento reverso, a utilização de nomes completos é obrigatória. O domínio reverso *default* não é o domínio da organização, e sim um domínio do tipo x.in-addr.arpa. O domínio reverso *default* de um servidor que mapeia endereços da rede 200.120.10.0/24 é 10.120.200.in-addr.arpa. Portanto, se você utilizar nomes relativos ao domínio *default*, os mapeamentos reversos levarão a nomes de máquinas do domínio x.in-addr.arpa.

Se você usa o servidor DNS do Windows 2000 e atualiza os dados de seu domínio através do Gerenciador DNS (Iniciar > Programas > Ferramentas Administrativas > DNS), problemas deste tipo ocorrerão com menos freqüência. A interface gráfica oferecida não deixa que o nome completo da máquina seja inserido, apenas o nome relativo à zona sendo configurada. Os arquivos gerados pelo servidor usam sempre nomes relativos nos registros IN A e acrescenta automaticamente o nome do domínio direto nos registros IN PTR. Se você está modificando os arquivos de zonas manualmente, a probabilidade de erro é maior.

Sempre que adicionar ou modificar algum registro em arquivos de zonas lembre-se de testar a modificação. Por exemplo, suponha que você adicionou mais um servidor Web (www1.exemplo.com.br) nos arquivos de zona. Imediatamente após reiniciar o serviço DNS, teste-o:

```
root# nslookup
> www1
Server:         200.120.10.53
Address:        200.120.10.53#53
Name:   www1.exemplo.com.br
Address: 200.120.10.101
> 200.120.10.101
Server:         200.120.10.53
Address:        200.120.10.53#53
101.10.120.200.in-addr.arpa     name = www1.exemplo.com.br.
```

Este teste comprova que as modificações realizadas foram corretas e que o servidor já as reconhece.

7.7 Filtro IP barrando tráfego DNS

7.7.1 Descrição

Leia mais sobre DNS no apêndice 10

Se existir um filtro IP barrando o tráfego DNS em sua organização você enfrentará sérios problemas. Um filtro pode estar barrando o tráfego entre seu servidor DNS e os clientes DNS deste servidor, entre servidor primário e servidores secundários ou entre servidores DNS internos de sua organização e servidores DNS que não pertencem a sua organização.

O primeiro caso é bastante raro, pois não é comum que exista um filtro IP entre os clientes DNS e o servidor destes clientes. Mas, se existir e não estiver permitindo a passagem do tráfego DNS, o resultado drástico: os clientes DNS não conseguirão se comunicar com o servidor e nenhum nome será resolvido para os clientes.

Servidores secundários precisam se comunicar com os servidores primários de tempos em tempos em busca de modificações nos arquivos de zonas. Se modificações foram realizadas no servidor primário, uma transferência das zonas modificadas é feita. Além disso, alguns servidores DNS estão configurados para notificar os servidores secundários quando modificações em zonas forem realizadas. Se um filtro IP barra a comunicação entre servidores primário e secundários, os servidores secundários não conseguirão se comunicar com o primário e após algum tempo deixarão de ter autoridade para resolver nomes do domínio que não pode ser atualizado, até que a comunicação seja novamente possível.

Por fim, é possível que exista um filtro IP mal configurado barrando o tráfego entre servidores internos da organização e servidores de outras organizações. A

conseqüência será que nomes não locais nunca poderão ser resolvidos pelo servidor de nomes da organização.

Em muitas organizações, a arquitetura DNS apresentada na Figura 7-2 é empregada. Nesta arquitetura existe um servidor DNS externo, responsável pela resolução dos nomes públicos da organização e um servidor DNS interno. As máquinas clientes da organização usam o servidor DNS interno, que está protegido por um *firewall*. Nenhum servidor DNS fora da organização precisa consultar o servidor DNS interno. No entanto, o servidor DNS interno precisa se comunicar com o servidor DNS externo para resolver nomes para seus clientes DNS. Este é um exemplo em que existe um filtro IP entre servidores DNS.

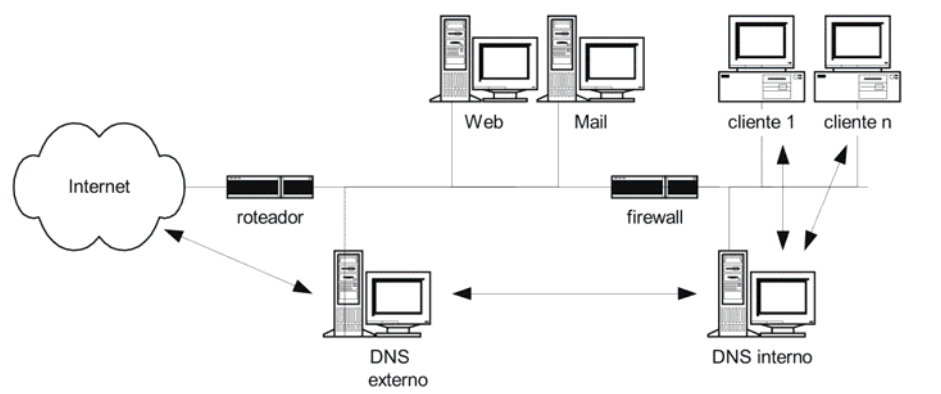



Figura 7-2: Arquitetura DNS de separação de função.

O serviço DNS usa as portas TCP/53 e UDP/53. A maioria das pesquisas feitas por clientes é destinada à porta UDP/53 do servidor DNS. No entanto, mensagens UDP são restritas a um tamanho de 512 bytes. Portanto, pesquisas cujas respostas são maiores que este tamanho são novamente realizadas via o protocolo TCP [RFC1035, RFC2181]. Além disso, transferências de zonas são feitas utilizando o protocolo TCP, que é confiável. Desta forma, não basta permitir apenas a passagem de tráfego UDP/53 para os servidores DNS. É preciso também permitir o tráfego TCP/53.

Nas versões mais antigas do BIND (anteriores a 8.1) um servidor de nomes de domínio sempre usava a porta de saída UDP 53 para consultar outros servidores. No entanto, a partir desta versão, uma porta entre 1024 e 65535 é escolhida randomicamente pelo servidor DNS. Se um filtro IP estiver configurado para aceitar consultas externas apenas se a origem estiver na porta UDP (ou TCP) 53, o tráfego entre servidores de nomes vai ser barrado.

7.7.2 Sintomas

Se o filtro IP não permite a comunicação entre o servidor DNS da organização e outros servidores DNS (inclusive o servidor externo), a resolução de nomes não locais não será possível. Os usuários reclamarão que não conseguem acessar qualquer serviço fora da organização. Provavelmente reclamarão que não conseguem acessar páginas na Internet e não conseguem receber nem enviar mensagens de/para usuários externos. O navegador vai informar ao

usuário um erro de DNS. No Internet Explorer, por exemplo, após algum tempo, uma página de erro é apresentada, contendo mensagens como: "`Não é possível encontrar <nome-da-maquina>`" ou "`A página não pode ser exibida (…) Não é possível encontrar o servidor ou ocorreu um erro de DNS`".

Quando o tráfego DNS entre o servidor primário e os secundários é barrado (por exemplo o tráfego TCP/53 não é permitido entre eles) os servidores secundários ficarão desatualizados e após um certo tempo (expiração) não mais responderão pelo domínio. Os clientes DNS destes servidores ficarão sem resolução de nomes e reclamarão que a rede não está funcionando, já que a maioria dos serviços é acessada através do nome do servidor. O mesmo ocorre quando o tráfego DNS é barrado entre o servidor DNS e os clientes DNS. O navegador dos usuários informará o erro de DNS.

Se o filtro estiver barrando o tráfego do servidor DNS que resolve nomes públicos da organização, usuários externos se queixarão de não conseguir acessar os serviços de sua organização: enviar *e-mails*, por exemplo.

7.7.3 Sinais

Procedimento **12.4**

Consultas DNS sem resposta. Duas situações podem ocorrer: 1) a própria consulta é barrada por um filtro IP e não chegará até o servidor DNS destino ou 2) a resposta dada não passa pelo filtro IP, não podendo chegar até o cliente ou servidor que solicitou a consulta.

Procedimento **12.3**

A resolução de nomes externos não funciona. Este pode ser um sinal de que o tráfego DNS entre seu servidor de nomes e servidores de nomes de outras organizações (ou até mesmo o servidor de nomes externo da organização) está sendo barrado por um filtro IP.

Procedimento **12.2**

Nos servidores secundários mensagens no arquivo de *logs* indicam que não foi possível a comunicação com o servidor principal. Este pode ser um sinal de que o tráfego entre servidores secundários e principais está sendo barrado por um filtro IP.

7.7.4 Testes confirmatórios

Este problema causa os mesmos sinais do problema **O SERVIÇO DE NOMES NÃO ESTÁ HABILITADO**. Antes de realizar o teste a seguir, certifique-se de que o servidor de nomes está em execução. Isto pode ser feito como descrito nos testes confirmatórios da página 171 ou pode ser feito simplesmente com o comando a seguir:

```
# telnet <IP do servidor DNS> 53
```

Se o servidor DNS responder, ele está em execução.

RESUMO DOS TESTES

TESTE 1

Localize os filtros IP da organização localizados entre servidores DNS e verifique se eles permitem a passagem do tráfego DNS;

Teste confirmatório 1

Se existirem filtros IP entre os servidores de nomes de sua organização ou entre eles e servidores DNS fora da organização, verifique a configuração do filtro.

As regras que deverão estar contidas no filtro IP sendo analisado dependem de onde o filtro se localiza. Ele está entre o servidor de nomes interno e o externo? Entre o servidor primário e secundários? Você precisa conhecer o tráfego DNS que deverá passar pelo filtro e analisar se as regras de filtragem estão corretas.

Lembre-se que servidores DNS mais novos usam uma porta não bem conhecida (entre 1024 e 65535) para realizar consultas em outros servidores, enquanto os mais antigos usam a porta de saída UDP/53. Considere ainda que, algumas consultas que geram respostas maiores que 512 bytes se tornam consultas TCP.

Se você perceber que não é permitida a passagem do tráfego para a porta TCP/53 ou UDP/53 de servidores ou desta porta para portas não bem conhecidas de clientes ou outros servidores, o problema foi confirmado.

Considere novamente o exemplo apresentado na Figura 7-2. Você percebeu que os servidores de nomes internos não conseguem resolver nomes não locais. Você resolveu analisar as regras do filtro IP no *firewall* e percebeu que a passagem do tráfego com destino à porta UDP/53 não está sendo permitida. Resultado: os servidores DNS internos não conseguem se comunicar com os servidores de nomes externos para resolver nomes não locais.

Para verificar as regras de filtragem em um ambiente Linux usando `ipchains` ou `iptables` use um dos seguintes comandos:

```
# ipchains –L –n | more

# iptables –L –n | more
```

Em um roteador Cisco com listas de acesso configuradas use o comando:

```
roteador# show access-list
```

7.7.5 Sugestões de tratamento

Se o problema foi confirmado, corrija as regras de filtragem do *firewall*. Lembre-se que tanto o tráfego TCP/53 quando UDP/53 devem ser permitidos. Analise que tipo de tráfego DNS vai atravessar o filtro IP (entre servidor primário e secundários, entre servidores interno e externos, entre servidores e clientes) e reajuste as regras do filtro para corrigir o problema.

É mais comum que o *firewall* barre o tráfego entre servidores internos e servidores externos (que não estão sob sua administração), ou que você esqueça de permitir a passagem do tráfego TCP/53. Abaixo são ilustradas estas situações mais comuns de ocorrência deste problema e como solucioná-las:

1. filtro IP só permite a passagem de tráfego DNS quando a porta origem e a porta destino são UDP/53 (ou TCP/53). Você atualizou a versão do BIND dos servidores DNS e agora eles usam portas não bem conhecidas (isto é, maiores que 1023) para consultar outros servidores. O tráfego entre os servidores da organização e servidores fora dela será barrado.

a) opção 1: configure o servidor de nomes para novamente usar apenas a porta fonte 53 ao consultar outros servidores. Para tal adicione a opção em destaque a seguir nos servidores de nomes da sua organização:

```
options {
    directory "/var/named";
    query-source address * port 53;
};
```

Com esta opção o servidor de nomes passa a novamente usar a porta origem 53 ao consultar outros servidores. Note que esta solução é específica da implementação BIND.

b) opção 2: reconfigure as regras do filtro IP para permitir a comunicação entre servidores DNS internos, porta UDP(TCP)/1024-65535 e servidores externos porta UDP(TCP)/53.

Em um filtro IP Linux que usa `ipchains` adicione as seguintes regras:

```
DNS = "192.168.1.53" # endereço IP de um servidor DNS

any = "0.0.0.0/0.0.0.0"

ipchains -A forward -s $DNS 1024-65535 -d $any 53 -p tcp \
-j ACCEPT

ipchains -A forward -s $DNS 1024-65535 -d $any 53 -p udp \
-j ACCEPT

ipchains -A forward -s $any 53 -d $DNS 1024-65535 -p tcp \
-j ACCEPT

ipchains -A forward -s $any 53 -d $DNS 1024-65535 -p udp \
-j ACCEPT
```

Em um filtro IP Linux que usa `iptables` as regras são as seguintes:

```
DNS = "192.168.1.53" # endereço IP de um servidor DNS

any = "0.0.0.0/0.0.0.0"

iptables -A FORWARD -p tcp -s $any –sport 53 -d $DNS \
--dport 1024:65535 -j ACCEPT
```

```
iptables -A FORWARD -p tcp -s $any –sport 53 -d $DNS \
--dport 1024:65535 -j ACCEPT

iptables -A FORWARD -p tcp -s $DNS –sport 1024:65535 -d \
$any --dport 53 -j ACCEPT

iptables -A FORWARD -p udp -s $DNS –sport 1024:65535 -d \
$any --dport 53 -j ACCEPT
```

As regras descritas acima devem ser definidas para cada um dos servidores internos, não apenas para o servidor cujo IP é DNS. Elas devem substituir a antiga regra que permitia a passagem de tráfego quando as portas fonte e destino eram 53.

Se o filtro está configurado em um roteador Cisco substitua as antigas regras pelas regras a seguir na lista de acesso adequada:

```
access-list 102 permit tcp <DNS1> gt 1023 any eq domain
access-list 102 permit udp <DNS1> gt 1023 any eq domain
access-list 102 permit tcp any eq domain <DNS1> gt 1023
access-list 102 permit udp any eq domain <DNS1> gt 1023
```

Onde:

- 102 é o exemplo o número da lista de acesso sendo configurada. No seu caso use o número da sua lista de acesso. Listas de acesso estendidas (como as apresentadas) são identificadas por números entre 100 e 199 ou entre 2000 e 2699;

- <DNS1> deve ser substituído pelo endereço IP de um servidor de nomes interno. As regras apresentadas devem existir para todos os servidores de nomes internos.

As regras apresentadas acima são aplicáveis em um firewall que separe os servidores internos da organização (que servem aos clientes DNS locais) dos servidores DNS externos (que respondem pelos nomes públicos). Caso você não esteja utilizando esta arquitetura DNS, adicione também regras que permitam que servidores DNS fora da organização consultem seus servidores DNS. Neste caso, seus servidores é que estarão utilizando a porta 53 e os demais uma porta não conhecida ou a porta 53 (protocolos UDP ou TCP).

c) opção 3: adquira um *firewall* que conheça protocolos de camada de aplicação. Este *firewall* pode ser configurado para permitir a passagem de mensagens para o servidor de nomes apenas se os dados contidos nas mensagens são do protocolo DNS. Exemplo de um *firewall* que conhece protocolos de aplicação é o FireWall-1 da Checkpoint.

2. Você acabou de configurar o filtro IP e esqueceu de adicionar a regra para permitir a passagem do tráfego TCP/53. Adicione a regra para permitir a passagem deste tráfego. Os comandos a serem executados são bastante semelhantes aos comandos apresentados na opção 2 de solução da situação anterior.

7.8 Servidor de correio eletrônico com repasse totalmente aberto

7.8.1 Descrição

Leia mais sobre o serviço de correio eletrônico no apêndice 11

Diz-se que um servidor SMTP (*Simple Mail Transfer Protocol*) está com repasse (*relay*) aberto (também chamado *third-party relay* e *relay* inseguro) quando ele aceita transmitir uma mensagem de qualquer remetente na Internet para qualquer destinatário na Internet. Um servidor SMTP só deve aceitar transmitir um *e-mail* para um destino nas duas seguintes situações:

o destino é um usuário de um domínio para o qual o servidor está configurado para oferecer o serviço SMTP. Por exemplo, o servidor mail.exemplo.com.br está provavelmente configurado para fazer entregas de mensagens a usuários do domínio exemplo.com.br, como por exemplo, maria@exemplo.com.br;

o endereço IP do cliente que enviou a mensagem (independente dos destinatários) faz parte da faixa de endereços configurados como clientes SMTP do servidor.

Servidores de correio com repasse aberto são geralmente explorados por *spammers* – pessoas que enviam *e-mails* não solicitados em grande quantidade. Por que *spammers* usam servidores SMTP com repasse aberto [MAPS-TSI]? Porque ao usar um servidor de correio com repasse inseguro o *spammer* pode enviar quantas mensagens quiser, para quaisquer destinatários, sem custos e no completo anonimato.

A organização que possui um servidor SMTP com repasse aberto é bastante prejudicada: ela tem seus recursos computacionais e de rede roubados e, além disso, é o nome dela que aparece nas “mensagens-lixo” enviadas pelos *spammers*.

Servidores SMTP com repasse aberto podem ser denunciados a organizações que lutam contra o *spam*. Nestas organizações existem bancos de dados onde são cadastrados os servidores que, comprovadamente, estão com repasse aberto. O MAPS (*Mail Abuse Prevention System*), por exemplo, é uma organização sem fins lucrativos cujo principal objetivo é defender o sistema de correio eletrônico da Internet de *spammers* [MAPS]. O MAPS *Relay Spam Stopper* (RSS) [MAPS-RSS] é uma base de dados baseada em nomes de domínio DNS onde estão listados servidores com repasse aberto. No Brasil não existe um órgão que regulamente ou puna *sites* com repasse aberto [ANTISPAM-BR]. No entanto, servidores brasileiros podem perfeitamente ser cadastrados em listas negras internacionais, como o MAPS RSS, por exemplo.

A tendência atual é que cada vez mais cada organização se proteja de *spammers* não possuindo servidores SMTP com repasse aberto e não aceitando *e-mails* de servidores SMTP abusivos. Os servidores de correio eletrônico podem ser configurados para consultar bancos de dados de servidores com repasse inseguro e não aceitar mensagens vindas de servidores que estão nestas listas negras. Com isso, mensagens vindas de um *site* abusivo serão sempre barradas, tenham sido elas enviadas ou não por *spammers*. Percebe o que ocorrerá se seu

servidor SMTP estiver cadastrado em uma base de dados de repasses abertos? Usuários de organizações que usam esta base de dados não receberão mensagens de usuários de sua organização.

7.8.2 Sintomas

Se seu *site* for cadastrado em bases de dados de repasses abertos os usuários locais reclamarão que não conseguem enviar mensagens para certos destinos (usuários cujo servidor SMTP estão configurados para consultar as listas negras de repasse aberto onde o seu servidor está cadastrado). Além disso, as mensagens enviadas podem retornar para os remetentes com mensagens de erro que indicam que o seu servidor SMTP está cadastrado em uma lista negra antispam.

Por exemplo, considere que o servidor mail.exemplo.com.br está cadastrado no MAPS RSS. Considere também que o servidor mail.cisco.com está configurado para consultar a base de dados MAPS RSS e não aceitar mensagens dos servidores que estão listados nela como inseguros. Os *e-mails* enviados de maria@exemplo.com.br para cris@cisco.com não serão entregues a Cris. Além disso, o servidor SMTP da Cisco devolverá a Maria a mensagem que ela transmitiu anexada a uma mensagem de erro do MAPS RSS. No conteúdo deste *e-mail* haverá um link para a página http://work-rss.mail-abuse.org/rss/enduser.html.

O administrador da rede receberá por *e-mail* avisos de outras organizações ou de organizações que lutam contra *spam* alertando-o sobre repasse aberto. Em geral essas mensagens são destinadas a postmaster@domínio ou abuse@domínio.

7.8.3 Sinais

Procedimento

12.8

O servidor SMTP aceita fazer a entrega de mensagens sempre, mesmo quando o endereço IP do cliente SMTP que solicitou a entrega da mensagem não é da rede interna e o destinatário não é um usuário local. Considere o servidor SMTP mail.exemplo.com.br. Ele deveria aceitar apensa fazer entregas solicitadas por clientes da rede local (192.168.1.0/24) ou entregas de mensagens destinadas a usuários da rede local (maria@exemplo.com.br, por exemplo). Se mail.exemplo.com.br aceitar entregar um *e-mail* para um cliente na máquina 200.120.1.2 para cris@cisco.com, certamente, o servidor SMTP em questão está com repasse aberto.

7.8.4 Testes confirmatórios

O sinal apresentado na seção anterior é confirmatório, não sendo necessários outros testes adicionais.

7.8.5 Sugestões de tratamento

Para corrigir o problema o servidor SMTP com repasse aberto deverá ser atualizado para uma versão mais segura, ou deve ter sua configuração alterada para tornar-se um servidor com repasse seguro.

As implementações mais novas do `sendmail` (v8.9 e superior), assim como a implementação `qmail` do serviço SMTP negam repassar qualquer mensagem por *default*. Isto lhe obriga a configurar corretamente o servidor para aceitar repassar as mensagens de/para usuários locais, isto é, configurar o repasse seletivo.

A melhor sugestão para corrigir este problema é atualizar o seu servidor SMTP para a versão mais nova possível e configurá-lo corretamente com repasse seletivo (ver Seção **SUGESTÕES DE TRATAMENTO** do problema **SERVIDOR DE CORREIO ELETRÔNICO COM REPASSE TOTALMENTE FECHADO** (página 205).

Se a atualização não for possível você terá que alterar algumas configurações do servidor SMTP para torná-lo seguro. Em [MAPS-TSI-FIX] encontram-se informações sobre como proceder para resolver o problema de repasse aberto em diversas implementações do servidor SMTP. Verifique qual a implementação e versão do seu servidor SMTP e proceda como descrito neste documento.

Ao receber mensagens que denunciam servidores SMTP sob sua administração de estarem com repasse aberto aja imediatamente: teste se o servidor está realmente com este problema e, sendo ele confirmado, corrija-o o mais rapidamente possível. Não espere entrar em uma lista negra ou começar a receber mais de 10 reclamações por dia para começar a agir.

Além do MAPS, existem outras organizações que lutam contra *spam*. Dentre elas encontram-se: ORDB (Open Relay DataBase), Osirusoft (OsiruSoft's Open Relay Spam Stopper) e Fabel (Fabel - Åbne mail relays). Ao fechar um repasse aberto, verifique nas listas destas organizações se o seu servidor está cadastrado como repasse aberto. Se estiver notifique-as da correção para que o seu servidor seja removido dos bancos de dados de servidores SMTP com repasse aberto. Após a notificação o seu servidor vai ser testado por cada organização onde ele estava cadastrado e só será retirado da lista negra se os testes indicarem que ele não mais está com repasse aberto.

O SpamCop.net e Network Abuse Clearinghouse são organizações que oferecem serviços de reportagem de servidores SMTP com repasse aberto. É interessante que você cadastre seu endereço nestas organizações, para que reclamações sobre servidores em seu domínio sejam enviadas ao endereço correto. Se você receber mensagens não solicitadas pode usar estas organizações para denunciar o servidor que permitiu o envio destas mensagens.

7.9 Servidor de correio eletrônico com repasse totalmente fechado

7.9.1 Descrição

Leia mais sobre o serviço de correio eletrônico no apêndice 11

Com o intuito de diminuir a quantidade de *spam* enviado por servidores SMTP com repasse (*relay*) totalmente aberto, as novas implementações do serviço SMTP vêm, por *default*, com repasse totalmente fechado. O servidor só aceita transmitir mensagens de um usuário que esteja usando a máquina onde o servidor está instalado (o *localhost*). Alguns servidores ainda permitem que mensagens para usuários locais sejam enviadas, outros não.

A implementação `qmail`, desde suas versões mais antigas, já vem negando o repasse por *default*. As versões 8.9 e superiores do `sendmail`, uma das implementações mais usadas do serviço SMTP, também já apresentam este comportamento por *default*.

Se você vai atualizar a versão do seu servidor SMTP ou vai passar a utilizar outra implementação fique atento a este fato. Só coloque a nova versão em funcionamento quando tiver certeza absoluta de que o servidor não irá negar transmitir mensagens enviadas por ou destinadas aos próprios usuários locais.

7.9.2 Sintomas

Os usuários não poderão enviar e-mails, exceto se estiverem na máquina onde o servidor SMTP está instalado. Como os usuários usarão outras máquinas, eles reclamarão que não conseguem enviar mensagens, sejam elas locais ou não. Alguns servidores, por *default*, aceitam enviar mensagens destinadas a usuários locais, outros não. Mas, nenhum deles transmitirá mensagens destinadas a usuários não locais.

No cliente SMTP mensagens de erro serão apresentadas aos usuários. No Outlook Express da Microsoft, por exemplo, a seguinte mensagem será passada: “`A mensagem não pôde ser enviada porque um de seus destinatários foi recusado pelo servidor…`”.

7.9.3 Sinais

Procedimento **12.7**

O servidor SMTP não aceita enviar mensagens destinadas a usuários não locais, exceto para clientes usando a própria máquina onde o serviço está instalado. Ao tentar usar o serviço de qualquer outra máquina você observará o erro que indica repasse *denied*.

7.9.4 Testes confirmatórios

O sinal apresentado na seção anterior é confirmatório. Se ele for observado nenhum teste adicional precisa ser realizado.

7.9.5 Sugestões de tratamento

A configuração de repasse seletivo depende da implementação do serviço SMTP em uso. A seguir serão dadas dicas de como corrigir o problema em implementações `sendmail` e `qmail`.

No `sendmail` versões 8.8 e superiores, adicione o nome ou o IP das máquinas que podem ser clientes do servidor SMTP no arquivo /etc/mail/relay-domains. Informações sobre outras configurações encontram-se em [CONTROLLED-SMTP-RELAYING]. Por exemplo, suponha que você deseja que todos os usuários da rede 192.168.1.0/24 possam usar o servidor SMTP. Então, insira a seguinte linha no arquivo relay-domains:

```
192.168.1
```

Em seguida reinicie o `sendmail`. Apenas as versões 8.7 e superiores aceitam o sinal –HUP.

```
# killall –HUP sendmail
```

Ou, para os sistemas que não suportam o comando `killall`:

```
# kill -HUP <número do processo do sendmail53>
```

O `qmail` só aceita mensagens destinadas a máquinas listadas no arquivo /var/qmail/control/rcpthosts. Quando terminamos de instalar o `qmail`, este arquivo contém o nome da máquina local. Se o arquivo rcpthosts não existir, o `qmail` vai passar a ser repasse aberto. Para ser mais seletivo realize os passos a seguir:

1. você precisará usar um TCP *wrapper* (`inetd` ou `tcpserver`, por exemplo). Se você usa o `inetd`, a primeira ação é modificar a linha correspondente ao serviço SMTP (iniciada com smtp) no arquivo de configuração do `inetd` (/etc/inetd.conf). A nova linha deve ser a seguinte:

```
smtp stream tcp nowait qmaild /usr/local/bin/tcpd
/var/qmail/bin/tcp-env /var/qmail/bin/qmail-smtpd
```

A linha foi quebrada acima em duas, mas no arquivo inetd.conf tudo isso deve ficar em apenas uma linha.

2. reinicie o serviço `inetd`:

```
# kill –HUP <número do processo inetd>
```

3. por fim, insira as seguintes linhas no arquivo /etc/hosts.allow:

```
tcp-env: 192.168.1. : setenv = RELAYCLIENT
tcp-env: 0.0.0.0
```

A primeira linha configura a variável de ambiente RELAYCLIENT com um valor nulo para os clientes SMTP cujo endereço pertence à rede 192.168.1.0/24. Quando esta variável existe o arquivo rcpthosts é ignorado. Com isto, clientes

---

[53] Pode ser obtido com o comando # `ps –ae | grep sendmail`.

nestas máquinas podem usar o serviço SMTP para enviar mensagens para quaisquer destinos. A segunda linha permite que o serviço seja acessado por outros usuários que não pertencem à rede local (outros servidores de correio eletrônico, por exemplo), mas neste caso apenas mensagens destinadas a usuários dos domínios cadastrados como locais serão transmitidas.

Estas configurações são explicadas na FAQ do servidor qmail [QMAIL-FAQ]. Consulte-as para saber como proceder quando o `tcpserver` estiver sendo usado.

Nunca atualize e ponha no ar uma nova versão ou nova implementação do serviço SMTP sem antes ter lido algo sobre ela. Descubra se ela vem, por *default*, com repasse totalmente aberto ou totalmente fechado. Qualquer que seja o comportamento do servidor, você terá que modificá-lo. Certamente, você não quer um servidor que se nega a enviar mensagens sempre, e também não quer um que envie mensagens de quaisquer remetentes para quaisquer destinatários. Em geral, você quer configurar um repasse seletivo: o servidor aceita enviar mensagens externas apenas para clientes em determinadas máquinas.

Se você estiver com dúvidas sobre a nova versão ou a nova implementação, teste o novo servidor em uma máquina de testes. Organize os passos que devem ser seguidos até que ele se comporte como você deseja. O serviço SMTP é importante, tão importante quanto (ou mais importante) o serviço Web. Não corra o risco de interrompê-lo, exceto se estritamente necessário – o servidor foi invadido, por exemplo.

7.10 Referências

7.10.1 Livros

[DNS&BIND] Albitz, P. Liu, C. DNS and BIND. Quarta Edição. O'Reilly. Abril, 2001.

7.10.2 Recursos online (Internet)

[ANTISPAM-BR] Como denunciar e reclamar?

http://www.antispam.org.br/denunciar.html

[CONTROLLED-SMTP-RELAYING] Allowing controlled SMTP relaying in Sendmail 8.9.

http://www.sendmail.org/tips/relaying.html.

[MAPS] Site do Mail Abuse Prevention System (MAPS).

http://www.mail-abuse.org/

[MAPS-RSS] Site do MAPSSM Relay Spam Stopper (RSS).

http://work-rss.mail-abuse.org/rss/index.html

[MAPS-TSI] Rosenthal, C. What is Third-Party Mail Relay?

http://mail-abuse.org/tsi/ar-what.html

[MAPS-TSI-FIX] Rosenthal, C., Falk, J. D. How Can I Fix the Problem?

http://mail-abuse.org/tsi/ar-fix.html.

[QMAIL-FAQ] FAQ do servidor SMTP qmail.

http://www.qmail.org/qmail-manual-html/misc/FAQ.html

7.10.3 RFCs

[RFC1035] Mockapetris, V. Domain names - implementation and specification. Novembro, 1987.

[RFC1912] Barr, D. Common DNS Operational and Configuration Errors. Fevereiro, 1996.

[RFC2181] Bush, R., Elz, R. Clarifications to the DNS Specification. Julho, 1997.

[RFC2308] Andrews, M. Negative Caching of DNS Queries. Março, 1998.

7.10.4 Livros base

[DNS-WIN-2000] Larson, M., Liu, C. DNS on Windows 2000. Segunda edição. O'Reilly. Setembro, 2001.

[SENDMAIL] Costales, B. Allman, E. Sendmail. Segunda Edição. O'Reilly. Janeiro, 1997.

8 Os Índices Invertidos

Neste capítulo apresentamos dois índices invertidos: o índice invertido de sintomas e o índice invertido de sintomas e sinais. Estes índices podem lhe ajudar a criar sua lista de hipóteses (ver Seção **3.4 DESENVOLVA HIPÓTESES** na página 36).

8.1 Índice invertido de sintomas

O índice invertido de sintomas leva em consideração apenas os sintomas de um problema. Ele é interessante quando você não consegue coletar sinais de um problema. O índice invertido de sintomas é apresentado na Tabela 8-1.

Sintoma: Rede lenta
Cabo rompido ou danificado
Conector defeituoso ou mal instalado
Descasamento de modo de operação
Equipamento de interconexão defeituoso
Saturação de banda em segmentos Ethernet compartilhados
Placa de rede ou porta de equipamento de interconexão defeituosos
Violação de regras de cabeamento Ethernet
Tipo errado de cabo
Interferência no cabo
Saturação de recursos devido a excesso de quadros de difusão
Tempo de envelhecimento de tabelas de endereços inadequado
Validade da cache ARP inadequada
VLANs não estão configuradas
Tráfego RIP saturando largura de banda
TTL e outros campos do registro SOA com valores inadequados

Sintoma: Falta de conectividade[54]

[54] A falta de conectividade pode ser completa ou seletiva. No último caso, os usuários podem sentir falta de conectividade apenas para alguns servidores, o que será traduzido por eles como indisponibilidade de alguns serviços. Portanto, se os usuários reclamarem de indisponibilidade de alguns serviços, acrescente a sua lista os problemas cujo sintoma é falta de conectividade.

Cabo rompido ou danificado

Descasamento de modo ou velocidade de operação

Equipamento de interconexão defeituoso

Placa de rede ou porta de equipamento de interconexão defeituosos

Conector defeituoso ou mal instalado

Tipo errado de cabo

Interface desabilitada

Problema com árvore de cobertura

Saturação de recursos devido a excesso de quadros de difusão

Validade da cache ARP inadequada

Endereço IP de hospedeiro incorreto

Hospedeiro com máscara de rede incorreta

Servidor DHCP mal configurado

Rotas estáticas mal configuradas (em roteadores)

Equipamento inserido em VLAN incorreta

VLANs não estão configuradas

Comutadores não conseguem trocar informações sobre VLANs entre si

Ambiente RIP-1 com VLSM e/ou redes não contíguas

Diâmetro RIP muito grande

Roteadores RIP2 não enviam ou recebem pacotes RIP1

Filtro IP não permite a passagem de tráfego RIP (UDP 520)

O serviço de nomes não está habilitado

O TTL *default* de uma zona não está configurado

Filtro IP barrando tráfego DNS

Sintoma: Conectividade intermitente

Conector defeituoso ou mal instalado

Tempo de envelhecimento de tabelas de endereços inadequado

Endereço IP de hospedeiro incorreto

Servidor DHCP mal configurado

Sintoma: Falta de conectividade com algumas máquinas da rede local

O TTL *default* de uma zona não está configurado

Sintoma: Indisponibilidade de alguns serviços

Equipamento inserido em VLAN incorreta

VLANs não estão configuradas

Comutadores não conseguem trocar informações sobre VLANs entre si

O número de série não foi aumentado

TTL e outros campos do registro SOA com valores inadequados

Descasamento de registros A e PTR em arquivos de zonas DNS

Falta "." após nomes totalmente qualificados em registros DNS

Sintoma: Precisa esperar algum tempo para que a conexão com o servidor seja

estabelecida
Descasamento de registros A e PTR em arquivos de zonas DNS
Sintoma: Não consegue enviar e-mails
Servidor de correio eletrônico com repasse totalmente fechado
Sintoma: Não consegue enviar e-mails para certos destinos
Servidor de correio eletrônico com repasse totalmente aberto

Tabela 8-1: Índice invertido de sintomas.

8.2 Índice invertido de sintomas e sinais

Na Tabela 8-2 apresentamos o índice invertido de sintomas e sinais de problemas.

Sintoma: Rede lenta
Sinais: Taxa elevada de erros
Cabo rompido ou danificado
Descasamento de modo e/ou velocidade de operação
Interferência no cabo
Conector defeituoso ou mal instalado
Placa de rede ou porta de equipamento de interconexão defeituosas
Tipo errado de cabo
Sintoma: Falta de conectividade
Sinais: Taxa elevada de erros
Cabo rompido ou danificado
Conector defeituoso ou mal instalado
Placa de rede ou porta de equipamento de interconexão defeituosas
Tipo errado de cabo
Sintoma: Conectividade intermitente
Sinais: Taxa elevada de erros
Interferência o cabo
Conector defeituoso ou mal instalado
Sintoma: Rede lenta
Sinais: Taxa elevada de erros Taxa elevada de colisões
Descasamento de modo e/ou velocidade de operação
Placa de rede ou porta de equipamento de interconexão defeituosas
Conector defeituoso ou mal instalado
Sintoma: Falta de conectividade
Sinais: Taxa elevada de erros

Taxa elevada de colisões

Placa de rede ou porta de equipamento de interconexão defeituosas

Conector defeituoso ou mal instalado

Sintoma: Rede lenta

Sinais: Taxa elevada de erros
- Taxa elevada de colisões
- Ocorrência de colisões tardias

Descasamento de modo e/ou velocidade de operação

Placa de rede ou porta de equipamento de interconexão defeituosos

Sintoma: Rede lenta ou falta de conectividade

Sinais: Equipamento não operacional
- Interfaces não operacionais
- Utilização de memória elevada
- Utilização de CPU elevada
- Tráfego de *broadcast/multicast* elevado

Equipamento de interconexão defeituoso

Sintoma: Rede lenta

Sinais: Taxa de colisões elevada
- Utilização de enlaces elevada

Saturação de banda em segmentos Ethernet compartilhados

Sintoma: Rede lenta ou falta de conectividade

Sinais: Taxa elevada de erros
- Taxa de colisões elevada
- Ocorrência de colisões tardias
- Quadros muito longos
- Tráfego elevado de *broadcast/multicast*
- Aumento da utilização de enlaces

Placa de rede ou porta de equipamento de interconexão defeituosas

Sintoma: Falta de conectividade, rede lenta ou conectividade intermitente

Sinais: Número elevado de erros
- Taxa elevada de colisões
- NEXT e atenuação

Conector defeituoso ou mal instalado

Sintoma: Rede lenta

Sinais: Taxa elevada de colisões
- Ocorrência de colisões tardias
- Atenuação

Violação de regras de cabeamento Ethernet

Sintoma: Rede lenta

Sinais: Taxa elevada de colisões

Ocorrência de colisões tardias

Violação de regras de cabeamento Ethernet

Placa de rede ou porta de equipamento de interconexão defeituosas

Descasamento de modo e/ou velocidade de operação

Sintoma: Falta de conectividade

Sinais: Inexistência de tráfego

Estado administrativo *down*

Interface desabilitada

Sintoma: Falta de conectividade

Sinais: Utilização elevada de CPU

Tempestade de enchente

Tempestade de quadros de difusão

Taxa elevada de colisões

Utilização elevada de enlaces

Problema com árvore de cobertura

Saturação de recursos devido a excesso de quadros de difusão

Sintoma: Rede lenta ou falta de conectividade

Sinais: Tráfego de *broadcast* elevado

Aumento da utilização de enlaces

Utilização elevada de CPU

Saturação de recursos devido a excesso de quadros de difusão

Sintoma: Rede lenta ou conectividade intermitente

Sinais: Ocorrência freqüente de enchentes

Aumento na utilização de enlaces

Tempo de envelhecimento de tabelas de endereços inadequado

Sintoma: Rede lenta (tempo pequeno) ou falta de conectividade temporária (tempo grande)

Sinais: Aumento da utilização de enlaces

Tráfego de difusão ARP elevado

Validade da cache ARP inadequada

Sintoma: Conectividade intermitente

Sinais: Duas respostas à mesma requisição ARP

Endereço IP de hospedeiro incorreto

Sintoma: Falta de conectividade

Sinais: Quadro de difusão enviados por máquinas de outra sub-rede

Endereço IP de hospedeiro incorreto

Servidor DHCP mal configurado

Sintoma: Falta de conectividade total ou para algumas máquinas da rede local

Sinais: Tráfego de mensagens ICMP de redirecionamento

Rotas específicas para outros hospedeiros

Requisições ARP sem resposta

Hospedeiro com máscara de rede incorreta

Servidor DHCP mal configurado

Sintoma: Conectividade apenas com máquinas da rede local

Sinais: Tráfego de mensagens ICMP de redirecionamento

Tabela de rotas de hospedeiros incorretas

Hospedeiro com máscara de rede incorreta

Sintoma: Falta de conectividade ou conectividade intermitente

Sinais: Mensagens no log indicam falta de IPs;

Existe conectividade via IP, mas não via nome DNS de máquina;

Tráfego de mensagens DHCPNAK;

Nenhuma requisição externa de clientes DHCP;

Requisições ARP sem resposta;

Tráfego de mensagens ICMP de redirecionamento;

Quadro de difusão enviados por máquinas de outra sub-rede;

Rotas específicas para outros hospedeiros;

DHCPREQUEST ou DISCOVER sem resposta.

Servidor DHCP mal configurado

Sintoma: Falta de conectividade

Sinais: Tráfego de mensagens ICMP de TTL excedido;

Tráfego de mensagens ICMP de destino inalcançável;

Crescimento rápido de ipOutNoRoutes.

Rotas estáticas mal configuradas

Sintoma: Falta de conectividade ou indisponibilidade de alguns serviços

Sinais: Requisições ARP sem resposta;

ICMP de destino inalcançável;

Tráfego de difusão originado em outra sub-rede;

Máquina com configurações de outra sub-rede;

Cliente DHCP com endereço IP 0.0.0.0.

Equipamento inserido em VLAN incorreta

Sintoma: Rede lenta, indisponibilidade de alguns serviços ou falta de conectividade

Sinais: Tráfego de difusão elevado;

Utilização de CPU elevada;

Utilização de enlaces elevada;

Tráfego de difusão originado em outra sub-rede;

Máquina com configurações de outra sub-rede.

VLANs não estão configuradas

Sintoma: Falta de conectividade ou indisponibilidade de alguns serviços

Sinais: Requisições ARP sem resposta;

DHCPREQUEST ou DISCOVER sem resposta;

Cliente DHCP com endereço IP 0.0.0.0.

Comutadores não conseguem trocar informações sobre VLANs entre si

Sintoma: Falta de conectividade

Sinais: Tráfego de mensagens ICMP de destino inalcançável.

Equipamento inserido em VLAN incorreta

Ambiente RIP-1 com VLSM e/ou redes não contíguas

Diâmetro RIP muito grande

Roteadores RIP2 não enviam ou recebem pacotes RIP1

Filtro IP não permite a passagem de tráfego RIP (UDP 520)

Sintoma: Rede lenta

Sinais: Utilização elevada de enlaces.

Tráfego RIP saturando largura de banda

Saturação de banda em segmentos Ethernet compartilhados

Sintoma: Falta de conectividade

Sinais: Tráfego ICMP de porta inalcançável;

Existe conectividade via IP, mas não via nome DNS de máquina.

O serviço de nomes não está habilitado

Sintoma: Indisponibilidade de alguns serviços

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina.

O número de série não foi aumentado

TTL e outros campos do registro SOA com valores inadequados

Falta "." após nomes totalmente qualificados em registros DNS

Sintoma: Indisponibilidade de alguns serviços

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina;

Servidores primário e secundários retornam respostas diferentes à mesma consulta.

O número de série não foi aumentado

TTL e outros campos do registro SOA com valores inadequados

Sintoma: Falta de conectividade apenas para a rede local ou completa

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina;

Log do servidor DNS indica "no default TTL".

O TTL *default* de uma zona não está configurado

Sintoma: Rede lenta

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina;

Servidores primário e secundários retornam respostas diferentes à mesma consulta.

TTL e outros campos do registro SOA com valores inadequados

Sintoma: Falta de conectividade

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina;

Resolução de nomes externos não funciona;

Logs dos servidores secundários;

Consultas DNS sem resposta.

Filtro IP barrando tráfego DNS

Sintoma: Alguns serviços não funcionam ou precisam esperar muito tempo para que a conexão seja estabelecida

Sinais: Resolução direta não casa com resolução reversa.

Descasamento de registros A e PTR em arquivos de zonas DNS

Sintoma: Indisponibilidade de alguns serviços

Sinais: Existe conectividade via IP, mas não via nome DNS de máquina;

Resoluções dão nomes duplicados do domínio.

Falta "." após nomes totalmente qualificados em registros DNS

Sintoma: Não conseguem enviar mensagens para certos destinos

Sintoma: Administrador recebe reclamações

Sinais: Servidor aceita fazer entrega sempre.

Servidor de correio eletrônico com repasse totalmente aberto

Sintoma: Não conseguem enviar mensagens

Sinais: Servidor não aceita repassar mensagens até mesmo para usuários locais.

Servidor de correio eletrônico com repasse totalmente fechado

Tabela 8-2: Índice invertido de sintomas e sinais.

Parte II
Catálogo de problemas

9 Procedimentos gerais

Os três primeiros procedimentos (apresentados no Capítulo 9) não são referenciados em problema algum. Por esta razão, são chamados procedimentos gerais. Eles informam como conectar um analisador de protocolos, como obter uma interface de linha de comando e como localizar problemas utilizando `ping` e `traceroute`. Estes procedimentos são, na realidade, procedimentos de apoio aos demais procedimentos.

9.1 Utilizando um analisador de protocolos

Em geral, o uso básico de um analisador de protocolos envolve três passos:

- conectar o analisador no local apropriado;
- criar filtros de captura que selecionem apenas o tráfego de interesse;
- capturar quadros e em seguida decodificá-los.

Neste procedimento abordaremos de forma geral cada uma destas etapas.

9.1.1 Conectando o analisador de protocolos

Quando desejamos capturar o tráfego de um enlace usando um analisador de protocolos, precisamos, primeiro, conectar o analisador adequadamente.

Antes de irmos adiante, é importante falarmos um pouco sobre *hubs* (traduzidos em todo este livro como repetidores) e comutadores. Um repetidor é um dispositivo eletrônico que opera no nível físico. Ele replica todo o sinal que chega em quaisquer de suas portas para todas as outras portas. Assim, quando conectamos um analisador de protocolos em um repetidor, o analisador será capaz de capturar o tráfego de todos os enlaces ligados ao repetidor.

Um comutador, por sua vez, opera em nível de enlace. Um comutador mantém em sua memória uma tabela de endereços que traz mapeamentos de endereços MAC em portas do comutador[55]. Quando um comutador recebe um quadro

[55] A tabela de endereços de um comutador é povoada da seguinte forma: quando o comutador recebe um quadro através de uma de suas portas, ele olha o endereço origem do quadro. Sabendo a porta por onde o quadro chegou o comutador simplesmente adiciona (ou atualiza) sua tabela de endereços com estas novas informações.

através de uma de suas portas ele verifica o endereço MAC destino do quadro. Em seguida ele pesquisa em sua tabela de endereços para qual de suas portas o quadro deve ser enviado. Se o mapeamento MAC ↔ porta desejado for encontrado em sua tabela de endereços, o quadro é transmitido apenas para a porta indicada na tabela de endereços. Apenas se o mapeamento não for encontrado na tabela de endereços o comutador enviará o quadro para todas as suas portas (*flooding*, traduzido aqui como enchente). Assim, quando conectamos um analisador de protocolos em um comutador, ele não será capaz de capturar o tráfego de todas as portas do comutador. O analisador capturará apenas os quadros de difusão do domínio de difusão ao qual está conectado, os quadros destinados a ele próprio e os quadros enviados por enchentes.

Um outro ponto que também deve ser levado em conta é a configuração das VLANs em um comutador. VLANs limitam domínios de difusão. É comum que na configuração *default* de um comutador todas as suas portas façam parte da mesma VLAN, chamada de VLAN *default*. Assim, se nenhuma outra VLAN for definida pelo administrador da rede, todas as portas do comutador farão parte do mesmo domínio de difusão, e assim, ao conectar o analisador em quaisquer de suas portas, todos os quadros de difusão serão capturados pelo analisador. Se outras VLANs forem definidas no comutador, um analisador conectado ao comutador será capaz de capturar apenas os quadros de difusão do domínio de difusão definido pela VLAN a que ele – o analisador – pertencer.

Por tudo já citado, podemos concluir que com o surgimento dos comutadores e em especial com sua ampla utilização, tornou-se mais difícil analisar o tráfego entre dois equipamentos da rede. Para deixar clara a diferença entre conectar um analisador de protocolos em um comutador e em um repetidor, veja a Figura 9-1 e a Figura 9-2 a seguir, retiradas de [CISCO-SPAN]. Nessas figuras, você deseja capturar o tráfego entre dois equipamentos ou duas redes A e B.

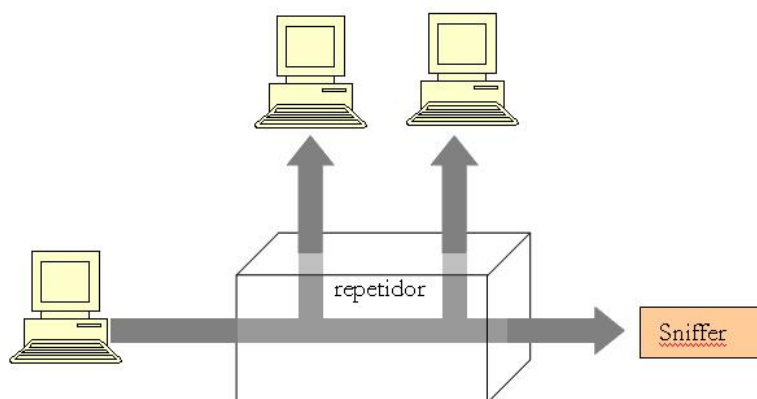



Figura 9-1: Analisador de protocolos conectado a um repetidor (*hub*).

Na Figura 9-1, o analisador está conectado a um repetidor. O tráfego originado na máquina A com destino à máquina B é transmitido para todas as portas do repetidor. O analisador conectado no repetidor será capaz, portanto, de capturar todo o tráfego entre as máquinas A e B. Já na Figura 9-2, o tráfego entre as máquinas A e B estará restrito às portas do comutador onde as máquinas A e B

estão conectadas[56]. Sendo assim, um analisador conectado ao mesmo comutador ao qual estão conectadas as máquinas A e B não será capaz de capturar o tráfego entre estas máquinas.

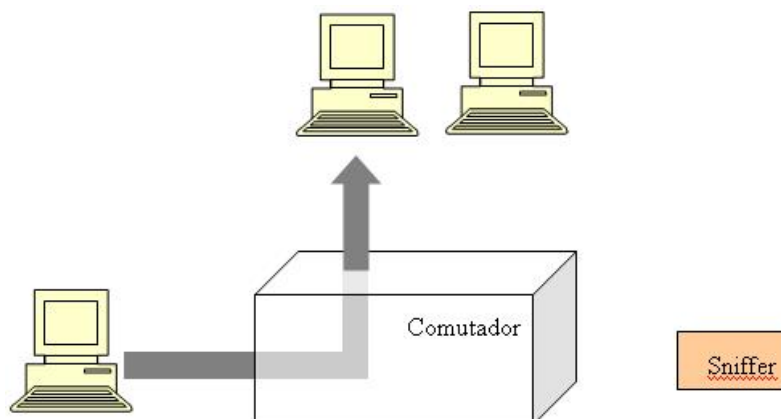



Figura 9-2: Analisador de protocolos conectado a um comutador (*switch*).

Para facilitar nossa vida, os comutadores mais novos oferecem uma funcionalidade conhecida como espelhamento de porta, monitoração de porta ou *Switched Port Analyzer* (SPAN). Podemos configurar os comutadores que oferecem esta funcionalidade para espelhar todo o tráfego de uma ou mais portas em uma outra porta, à qual conectamos o analisador de protocolos.

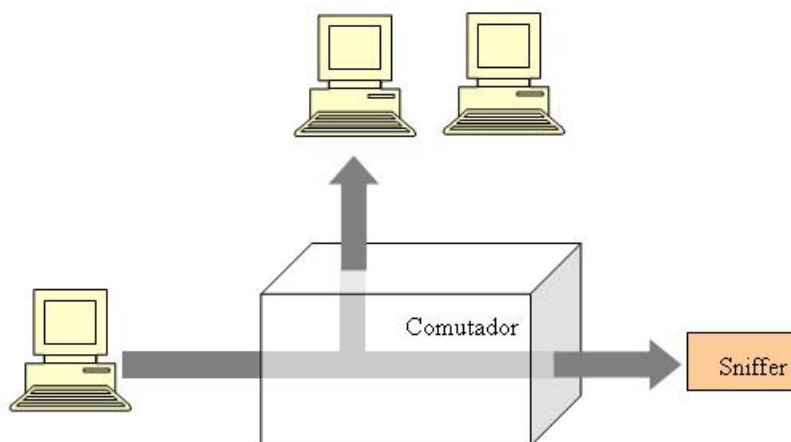



Figura 9-3: Comutador com função de espelhamento ativada.

Na Figura 9-3, retirada de [CISCO-SPAN], o comutador foi configurado para espelhar todo o tráfego da porta ligada à máquina B na porta ligada ao analisador de protocolos. Desta forma, o analisador de protocolos, apesar de estar conectado em um comutador, poderá enxergar todo o tráfego entre as máquinas A e B. Leia mais detalhes sobre a função de espelhamento e como configurá-la em comutadores Cisco em [CISCO-SPAN].

---

[56] Isto ocorrerá tão logo o comutador aprenda através de que portas as máquinas A e B são alcançáveis. Quando a máquina A transmitir um quadro pela primeira vez, o comutador aprenderá através de que porta a máquina A pode ser alcançada. O mesmo ocorrerá com a máquina B.

Quando desejamos analisar o tráfego entre dois equipamentos entre os quais existem apenas comutadores, a opção mais elegante é usar a função de espelhamento em um dos comutadores ligados aos equipamentos em questão. Mas, se a função de espelhamento não for oferecida pelos comutadores existentes entre os dois equipamentos, podemos ainda usar um repetidor auxiliar, como mostrado na Figura 9-4.

A utilização de um repetidor auxiliar envolve uma série de cuidados. O mais importante deles é que devemos assegurar que com a inserção do repetidor não causaremos descasamento de modo de operação na rede. Idealmente, enlaces que envolvem apenas comutadores e/ou roteadores devem operar no modo *full duplex*. Um repetidor, ao contrário, só é capaz de trabalhar no modo *half duplex*. Assim, a inserção do repetidor auxiliar pode causar descasamento de modo de operação. Para evitar este problema você deve configurar as portas dos equipamentos A e B ligadas ao repetidor para trabalharem no modo *half duplex*, ou configurá-las para o descobrimento automático do modo de operação. No último caso certifique-se de que o modo de operação *half duplex* foi configurado em ambas as portas dos equipamentos ligadas ao repetidor. Outro cuidado que devemos tomar é evitar o descasamento de velocidade de operação.

Quando usamos um repetidor auxiliar para conectar o analisador, além do descasamento de modo e velocidade de operação, o seguinte problema pode surgir: o tráfego, antes transportado por um canal *full duplex*, pode saturar o enlace que agora trabalha em modo *half duplex*. Se este for o caso a solução é adquirir um *splitter*. Ligue os equipamentos A e B ao *splitter* através de enlaces operando no modo *full duplex* e conecte o analisador de protocolos a outra porta do *splitter*. Com este equipamento você pode monitorar tráfego de enlaces *full duplex*. Apenas a função de monitoração passiva (sem geração de tráfego pelo analisador) pode ser realizada quando um *splitter* tiver sendo usado. Veja a ilustração na Figura 9-5.

Ao terminar a análise do tráfego, o repetidor auxiliar deve ser removido e as configurações originais de modo e velocidade de operação devem ser restauradas nas portas dos equipamentos às quais o repetidor foi conectado. Esta é uma forma alternativa e menos elegante de conectar um analisador em um ambiente totalmente comutado. Se já existir um repetidor entre os equipamentos cujo tráfego se deseja analisar, basta conectar o analisador neste repetidor.

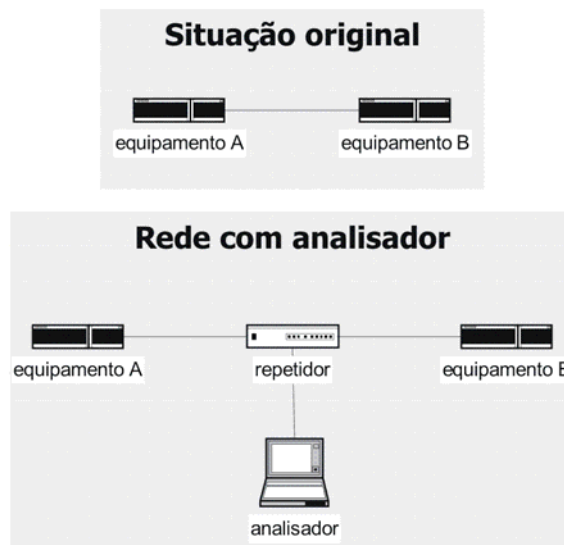



Figura 9-4: Conectando o analisador em um repetidor auxiliar.

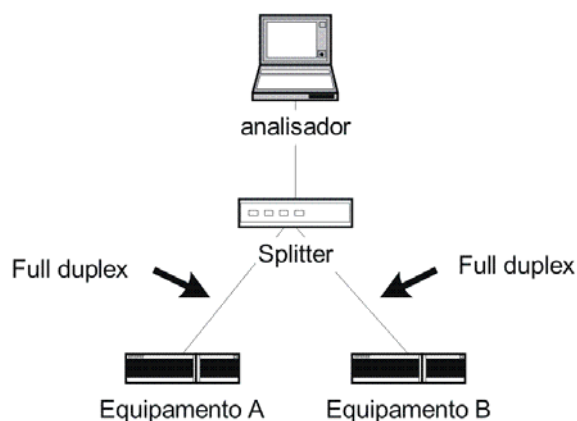



Figura 9-5: Conectando o analisador através de um *splitter*.

Muitas vezes desejamos analisar o tráfego que entra e/ou sai da organização. Em geral, existe um roteador de borda, que tem conexão com o mundo – um enlace de longa distância – e conexão com um roteador ou um comutador interno. Na Figura 9-6 mostramos um enlace por onde passa todo o tráfego originado ou destinado à Internet. Ao conectar um analisador que enxergue o tráfego deste enlace como mostrado anteriormente, podemos analisar o tráfego originado e destinado a redes externas.

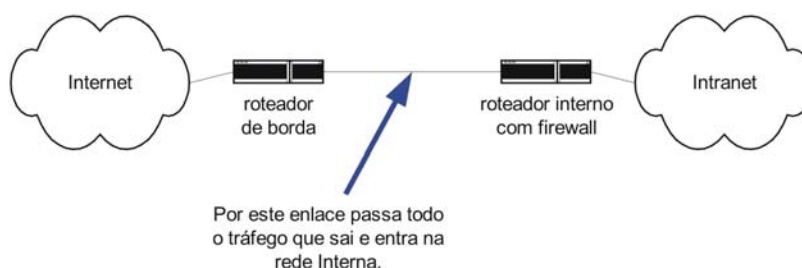



Figura 9-6: Enlace por onde passa todo o tráfego de entrada e saída da organização.

9.1.2 Criando e selecionando filtros de captura

Uma vez conectado o analisador em local apropriado, passamos para o passo dois: criar ou escolher filtros de captura para selecionar o tráfego capturado. Neste passo, utilizaremos como exemplo o analisador de protocolos Sniffer Pro v.3.5, da Network Associates. Em todos os procedimentos onde falamos sobre analisadores de protocolos usamos este analisador como exemplo.

A utilização básica deste analisador de protocolos é bastante intuitiva. Mostraremos aqui apenas algumas de suas funcionalidades básicas. Se o filtro desejado já foi criado, basta selecioná-lo na lista de opções em destaque na Figura 9-7.

Figura 9-7: Lista para seleção de filtro no Sniffer Pro v. 3.5.

Novos filtros de captura podem ser criados selecionando o item Define Filter do menu Capture. Quando escolhemos este item a caixa de diálogo de definição de filtro exibida na Figura 9-8 é apresentada.

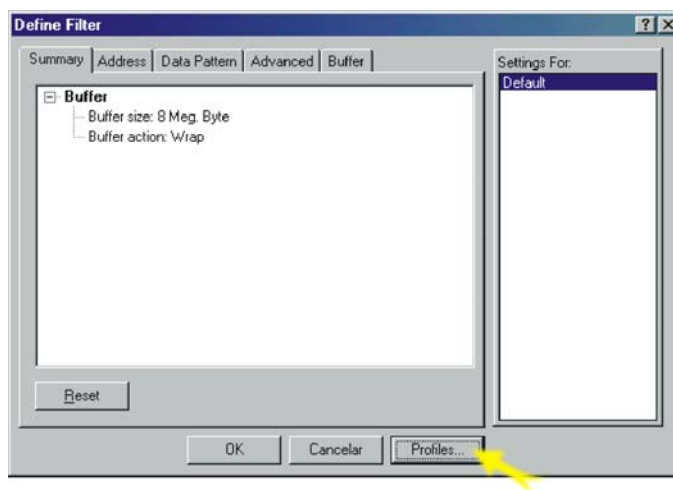



Figura 9-8: Janela para definição de filtro de captura no Sniffer Pro v. 3.5.

O filtro “Default” já existente captura todo o tráfego. Se você deseja criar um novo filtro, na janela de definição de filtro pressione o botão Profiles. A caixa de diálogo apresentada na Figura 9-9 surgirá. Então escolha criar um novo filtro pressionando o botão New. Em seguida, informe o nome do novo filtro de captura.

Ao criar filtros de captura escolha nomes sugestivos, que lhe lembrem que tipo de tráfego o filtro está configurado para capturar. Esta prática vai lhe ajudar a escolher rapidamente o filtro que você deseja quando muitos filtros já tiverem sido definidos. Nomear um filtro de captura com o nome filtro_1, por exemplo, não é uma boa prática. Por exemplo, se você estiver criando um filtro para

capturar o tráfego DHCP entre dois equipamentos, chame este filtro de "DHCP".

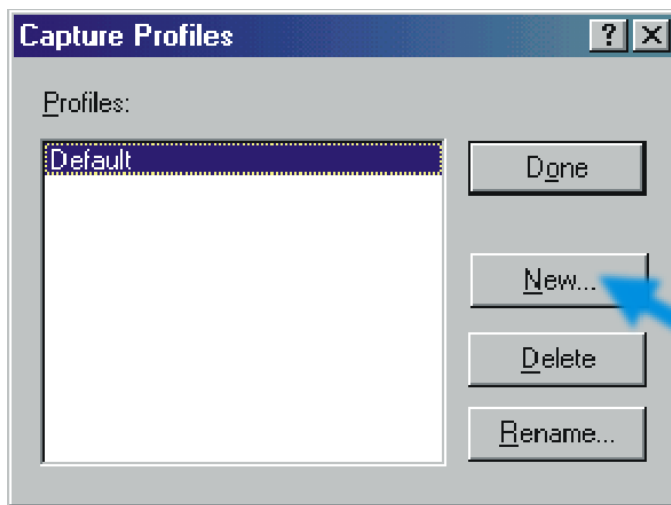



Figura 9-9: caixa de diálogo para a gerência de perfis de captura do Sniffer pro v. 3.5.

A mesma janela apresentada na Figura 9-8 surgirá, mas agora o filtro selecionado em Settings For é o novo filtro que você acabou de criar. Se você deseja apenas modificar um filtro já existente, selecione-o no painel Settings For e modifique-o como desejar usando as tabelas da janela de definição de filtro como descrito a seguir.

No Sniffer, assim como na maioria dos analisadores mais sofisticados, podemos criar filtros baseados em:

- endereços destino e origem dos quadros, tanto em nível de enlace (endereços MAC), quanto em nível de rede (endereços lógicos IP, IPX, etc.);

- padrões de dados. Neste caso, podemos selecionar um quadro já capturado com um certo padrão, por exemplo, uma mensagem ICMP do tipo 3, e criar um filtro com este padrão. Apenas mensagens ICMP tipo 3 (destino inalcançável) serão capturadas pelo filtro;

- protocolos conhecidos. Por exemplo, podemos facilmente criar um filtro que capture apenas quadros que contenham dados do protocolo DNS.

A criação de filtros baseados em endereços e protocolos é mais simples e em todos os procedimentos usaremos apenas estes tipos de filtros.

Para criar filtros baseados no endereço origem e/ou destino dos quadros ou datagramas, escolha a tabela Address na janela de definição de filtro. Nesta tabela, escolha o tipo de endereço no qual você quer basear o filtro. Na versão do Sniffer utilizada é possível escolher entre endereços de Hardware, IP ou IPX. Nesta tabela de endereços existe um painel contendo endereços conhecidos do tipo de endereço escolhido, que podem ser usados na definição do filtro.

Por exemplo, se você deseja criar um filtro que capture apenas quadros cujo endereço destino é de difusão nível 2, selecione o tipo de endereço Hardware, informe que quadros de qualquer endereço (any) para o endereço de difusão físico – Broadcast(FFFFFFFFFFFF) – devem ser considerados. Este endereço faz parte da lista de endereços físicos conhecidos. Arraste-o para a tabela de endereços. Veja como ficou a configuração do filtro na Figura 9-10.

Para criar filtros que capturem quadros de um ou mais protocolos, selecione a tabela Advanced Filter da janela de definição de filtro e escolha o protocolo desejado. Na Figura 9-11 mostramos a configuração de um filtro que captura apenas dados do protocolo DHCP. Na realidade você pode escolher quantos protocolos desejar. Por exemplo, você pode criar um filtro que capture dados do protocolo DHCP e DNS simultaneamente.

Além disso, você pode combinar a filtragem baseada em endereços com a filtragem baseada em protocolos e padrões de dados para formar um só filtro. É perfeitamente possível criar um filtro que capture apenas quadros contendo dados do protocolo DHCP originados em uma determinada máquina – o servidor DHCP, por exemplo.

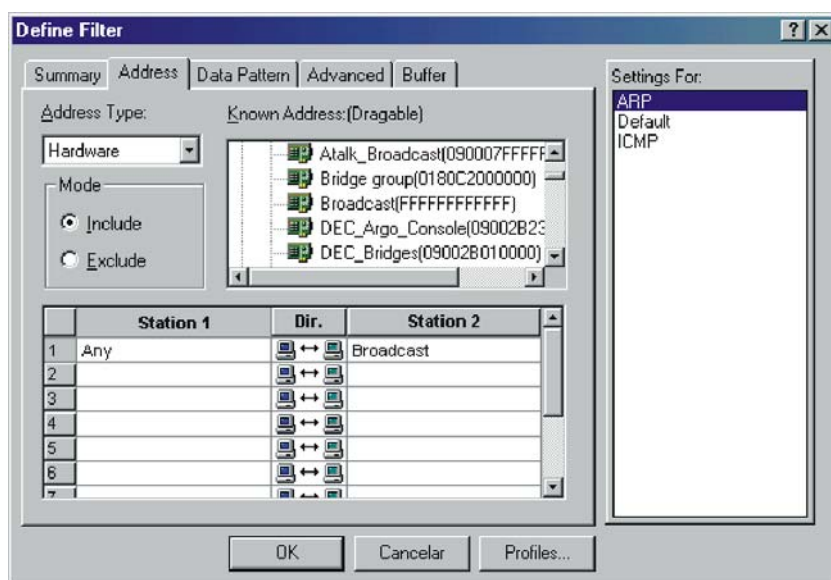



Figura 9-10: Configurando filtro baseado em endereços.

Em outros analisadores a criação de filtros não será muito diferente. Em alguns analisadores, alguns filtros já vêm criados por *default*. Quando criamos um filtro, ele fica selecionado e se imediatamente depois iniciarmos uma captura ele será usado.

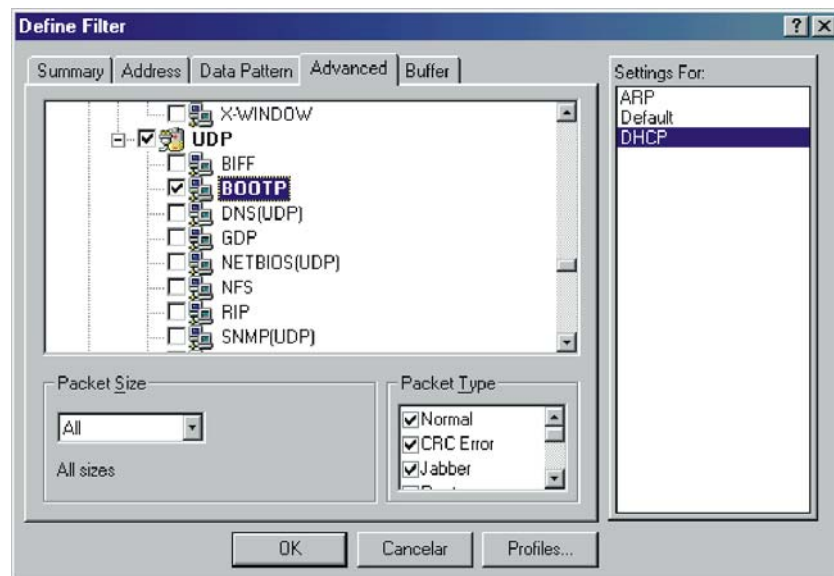



Figura 9-11: Definindo o protocolo cujos dados serão capturados.

9.1.3 Capturando e decodificando quadros

Enfim, chegamos ao último passo: capturar quadros e decodificar os quadros capturados. Mais uma vez, utilizaremos o analisador de protocolos Sniffer Pro v. 3.5, da Network Associates, como exemplo.

Após selecionar o filtro desejado, existem várias maneiras de iniciar uma captura no Sniffer. Dentre elas, encontram-se:

- pressione a tecla "F10";
- pressione o botão em destaque na Figura 9-12;
- no menu Capture escolha o item Start.

Figura 9-12: pressione este botão para iniciar uma captura no Sniffer pro v. 3.5.

Da mesma forma, podemos encerrar a captura de diversas maneiras:

- pressione a tecla "F9";
- pressione o botão em destaque na Figura 9-13;
- no menu Capture escolha o item Stop and display.

Figura 9-13: Pressione este botão para encerrar uma captura no Sniffer Pro v. 3.5.

Ao encerrar a captura a janela mostrada na Figura 9-14 será apresentada. Para ver os quadros capturados escolha a tabela Decode.

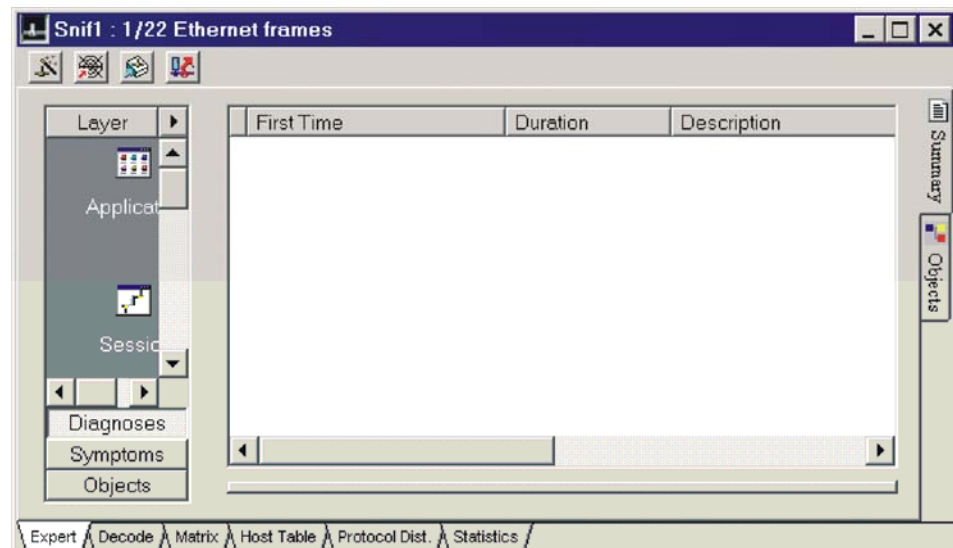



Figura 9-14: Janela apresentada após o encerramento de uma captura.

Nas demais tabelas desta janela encontramos outras informações bastante interessantes, como por exemplo as máquinas que mais transmitiram dados durante a captura.

9.1.4 Outras funções interessantes do Sniffer

Nem sempre precisamos capturar dados para descobrir sinais na rede. Quando o Sniffer começa a monitorar um enlace, ele apresenta estatísticas deste enlace em um painel. Veja este painel na Figura 9-15. Na tabela Details podemos ver outros detalhes do tráfego sendo monitorado. Veja o painel de detalhes na Figura 9-16. Estes painéis são bastante interessantes, e podem nos revelar rapidamente os sinais de um problema.

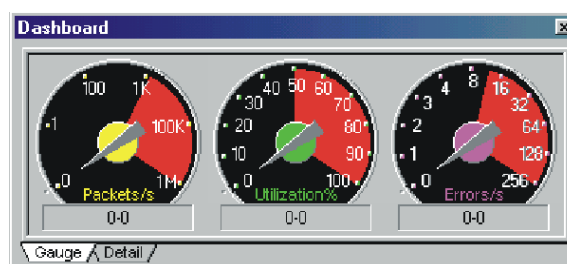



Figura 9-15: Painel de monitoração do Sniffer.

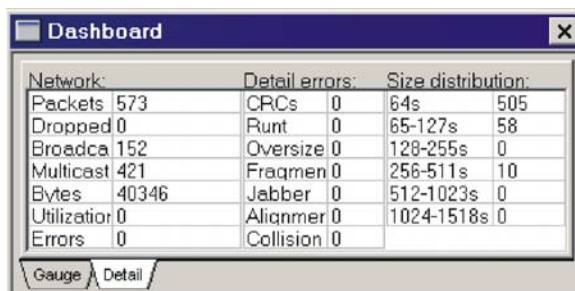



Figura 9-16: Painel com estatísticas de monitoração detalhadas do Sniffer.

Uma outra funcionalidade interessante do Sniffer é a de amostragem histórica (*History Samples*). O Sniffer pode gerar para você um gráfico que mostre certo tipo de tráfego no tempo. Podemos solicitar ao Sniffer, por exemplo, que gere um gráfico da quantidade de quadros de difusão por segundo. Para gerar este gráfico o Sniffer não precisa estar capturando quadros, apenas monitorando. Na Figura 9-17 apresentamos a janela para a configuração da amostragem histórica no Sniffer.

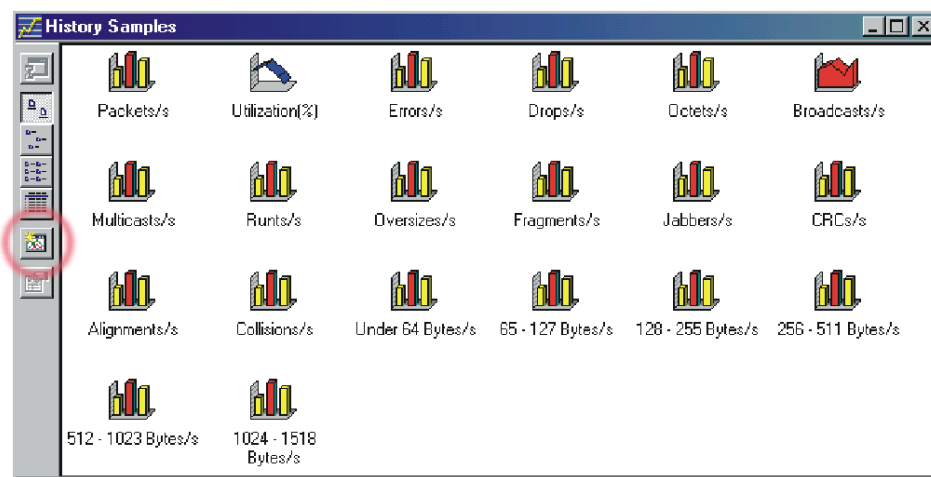



Figura 9-17: Janela para configuração da amostragem histórica no Sniffer.

Na Figura 9-17 podemos ver os tipos de gráficos que o Sniffer pode gerar. Pressionando o botão em destaque nesta mesma figura, podemos configurar gráficos que mostram múltiplas estatísticas, por exemplo, utilização e erros/s. Os passos a seguir podem lhe auxiliar a configurar o Sniffer a gerar um gráfico para você:

- selecione o item History Samples no menu Monitor, ou pressione o botão apresentado na Figura 9-18 no menu do Sniffer. A janela de amostras será aberta;

- na janela para a configuração da amostragem histórica informe o limiar para a estatística escolhida e o tipo do gráfico a ser gerado (se gráfico em linha, colunas, etc.). Nesta janela você pode também modificar o esquema das cores. Por *default*, quando o limiar for excedido o gráfico ficará vermelho;

- para criar um gráfico que apresente múltiplas medidas (de Jabbers/s e Oversizes/s, por exemplo), pressione o botão Add Multiple History apresentado em destaque na Figura 9-17. A janela para a configuração de um gráfico com múltiplas medidas surgirá;

- na tabela geral escolha um nome para o gráfico ("Jabbers/s e Oversizes/s", por exemplo) e o tipo do gráfico (linha, colunas, etc.). Na tabela de seleção exclua os itens que já estão selecionados por *default* (Packets/s, Utilization(%) e Error/s) e insira os itens Oversizes/s e Jabbers/s. Pressione o botão OK para salvar estas configurações;

- clique com o botão direito do mouse sobre o *history samples* que você acabou de configurar. No menu que surgir escolha o item Start Sample. O gráfico começará a ser traçado. Ele será atualizado a cada 15 segundos e caso você não finalize a amostragem manualmente, ela será encerrada após 15 horas.

Figura 9-18: Botão "History Samples".

Tudo o que falamos aqui são apenas funcionalidades básicas do Sniffer. No Sniffer existem muitas outras funcionalidades interessantes e mais sofisticadas que não exploramos. Se fossemos falar sobre cada função interessante do Sniffer teríamos que escrever outro livro.

Cabe a você e a sua equipe aprender a usar funcionalidades mais sofisticadas do seu analisador de protocolos a fim de obter dele as informações e o comportamento desejado.

9.1.5 Sobre analisadores de protocolos

Existem dois tipos de analisadores de protocolos: os analisadores dedicados e analisadores instalados em um computador pessoal. Os analisadores dedicados vêm em um *hardware* dedicado para a tarefa de análise. Eles são bastante caros, mas bastante profissionais e sofisticados. Estes analisadores de protocolos revelam informações detalhadas sobre a interface Ethernet, incluindo quadros com erros e ocorrência de colisões. É mais barato usar analisadores instalados em computadores pessoais, mas neste caso, para que o analisador possa detectar erros físicos e colisões será necessário comprar um adaptador de rede especial.

Por exemplo, o analisador de protocolos Sniffer da Network Associates (NAI), pode ser instalado em um computador pessoal com sistema operacional Windows ME. Ele funciona com praticamente todos os *drivers* de placas de rede. No entanto, apenas adaptadores avançados da NAI suportam todas as características do analisador, inclusive detecção de erros da camada física e colisões [SNIFFER_PRO-INSTALL]. *Drivers* comuns não repassam a informação

das camadas física e de enlace para o resto do sistema operacional. Assim, o analisador não toma conhecimento dos erros ocorridos.

9.2 Acessando a interface de linha de comando de um equipamento de interconexão

Em muitos outros procedimentos deste livro citamos comandos que podem ser executados em uma interface de linha de comando de um equipamento. Neste procedimento mostraremos como podemos obter acesso a esta interface em roteadores, comutadores e repetidores.

Existem duas formas de acessar a interface de linha de comando de um equipamento:

- através da porta de terminal (*console*) do equipamento;
- através de uma sessão de `telnet` para o equipamento.

Alguns repetidores menos sofisticados não oferecem uma interface de linha de comando. A seguir detalharemos cada uma destas formas de acesso.

9.2.1 Acesso através da porta *console*

Excetuando-se alguns repetidores mais pobres, todos os demais equipamentos de interconexão de rede têm uma interface, chamada geralmente *console* ou *management*, onde podemos conectar um terminal através de um cabo EIA/TIA-232 (RS-232).

Se você não possuir um terminal para conectar nesta interface, pode conectar um computador com software emulador de terminal como, por exemplo, `Hyper Terminal` e `pcplus`.

Ao conectar o terminal na porta RS/232, pressione a tecla **Return**. Será solicitado a você um *login* e uma senha para ter acesso à interface de linha de comando. Na realidade, nem todos os equipamentos pedem *login*. Você verá mais adiante que equipamentos Cisco pedem apenas a senha. Após fornecer o que é pedido, você poderá usar a interface de linha de comando do equipamento.

9.2.2 Acesso através de sessão de telnet

Para ser possível acessar a interface de linha de comando de um equipamento através de uma sessão de `telnet`, é necessário que este equipamento esteja configurado com um endereço IP.

Abra uma sessão de `telnet` com este equipamento a partir de uma máquina qualquer da rede. Por questões de segurança, é interessante que esta máquina esteja próxima do equipamento e que entre ela e o mesmo não existam

repetidores. Usando `telnet`, a senha que você digitar não é criptografada e alguém, com um analisador de protocolos, pode capturá-la na rede. O comando para abrir a sessão de `telnet` com o equipamento é:

```
# telnet IP_do_equipamento
```

Assim que iniciar a sessão você terá que informar um *login* (dependendo do fabricante do equipamento) e uma senha, para ter acesso à interface de linha de comando do equipamento.

Não existe uma padronização sobre a interface de linha de comando dos equipamentos de interconexão. Em geral elas são bastante semelhantes à interface não gráfica de sistemas Unix-*like*. Nas próximas sub-seções daremos algumas dicas de como lidar com as interfaces de linha de comando de equipamentos de interconexão. No entanto, como não há padronização, não podemos garantir que as dicas oferecidas serão válidas para quaisquer equipamentos.

9.2.3 Sobre logins e senhas

Você deve ter observado que independentemente de como a interface de linha de comando está sendo obtida, você terá que informar um *login* e uma senha. Na realidade, alguns equipamentos não solicitam *login*.

Equipamentos Cisco – roteadores e comutadores – por exemplo, pedem apenas uma senha. Após fornecermos a senha, ele oferece uma interface com comandos restritos, com os quais não é possível configurar o equipamento. O comando a seguir deve ser executado para que entremos no modo de configuração global (se necessário):

```
roteador> enable
```

Uma nova senha será solicitada. Após fornecê-la, estamos aptos a configurar o equipamento. Se estivermos apenas buscando informações sobre o equipamento não será necessário entrar no modo de configuração global do sistema. Neste livro, a maioria dos comandos apresentados não requer que você esteja o modo de configuração global.

Outros equipamentos solicitam um *login* e uma senha. Estes equipamentos vêm com usuários *default* criados. É interessante que você modifique a senha destes usuários tão logo receba o equipamento.

9.2.4 Dicas gerais de uso

Uma vez obtida a interface de linha de comando, algumas dicas são válidas:

- se após conectar o terminal no equipamento de interconexão você vir caracteres estranhos, é sinal de que a velocidade de comunicação entre o terminal e o equipamento não está ajustada. Em roteadores Cisco com IOS versão 10.0 ou superior a velocidade *default* de comunicação (transmissão e recepção) com o terminal é 9600 bps. Configure o seu

terminal com a mesma velocidade para que a comunicação seja possível. Uma vez obtida a interface de linha de comando, a velocidade de comunicação com o terminal. pode ser modificada com o comando:

```
roteador# terminal speed <nova velocidade>
```

- se você não sabe quais os comandos que estão disponíveis, use o *help* da interface de linha de comando, que pode geralmente ser obtido com o comando:

  ```
  roteador> ?
  ```

  Este comando oferece uma lista de todos os comandos que podem ser executados na interface obtida. Alguns equipamentos chegam a dar também uma pequena descrição de cada comando. Freqüentemente, o comando *help* pode ser usado também após um comando ainda incompleto, para que você saiba como pode completar o comando. Suponha que você deseja ver a configuração das interfaces de um roteador. Até agora já descobriu que deve usar um comando iniciado com a palavra show, mas, precisa saber como completar este comando. Então, o comando a seguir pode ajudar:

  ```
  roteador> show ?
  ```

  Este comando vai lhe mostrar todas as opções do comando `show`. Você pode usar o comando **?** em qualquer nível, para descobrir como construir o comando que você deseja;

- em muitos equipamentos não é necessário escrever todas as palavras do comando de forma completa. Basta escrever todas as iniciais até um ponto em que não haja mais a possibilidade de existirem dois comandos com as mesmas iniciais. Por exemplo, para ver todas as interfaces de um roteador Cisco podemos digitar os seguintes comandos:

  ```
  roteador> show interfaces
  ```

  Ou

  ```
  roteador> sh inter
  ```

  Ambos retornarão os mesmos resultados.

  Em outros equipamentos é necessário digitar o comando completo, mas o próprio equipamento pode terminar o comando para você. Basta que você escreva o início de uma palavra do comando e em seguida pressione a tecla de espaço e faça isso para todas as palavras que compõem o comando;

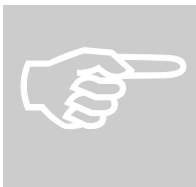
- excetuando os comandos do tipo `show`, que apenas apresentam na tela configurações do equipamento, se não tiver certeza sobre o que um comando faz, é melhor ler os manuais do equipamento antes de arriscar executá-lo. Uma interface de linha de comando é semelhante a uma interface não gráfica do Linux: não existe o comando "desfazer".

9.3 Localizando problemas com auxílio traceroute

Neste procedimento mostramos como usar `traceroute` para localizar problemas em uma rede.

9.3.1 Descrição e Dicas

Quando uma estação de gerência estiver sendo usada, ela indicará problemas através de alarmes. Outros eventos que não gerem alarmes também podem ser descobertos ao analisar as estatísticas apresentadas pela estação de gerência. No entanto, nem todos os elementos da rede são monitorados. Tipicamente, apenas os elementos mais críticos, em especial aqueles que participam do *backbone*, são monitorados pela estação de gerência. Isto exclui, muitas vezes, repetidores e/ou comutadores que estejam ligadas apenas a máquinas clientes.

Quando um problema ocorrer em um elemento da rede não monitorado, ele será provavelmente descoberto através de reclamações de um ou mais usuários. A ferramenta `traceroute` pode nos ajudar a localizar o problema.

Se nenhum elemento de sua rede está sendo monitorado através de uma aplicação de gerência, todos os problemas serão descobertos através dos usuários e isto não é uma boa prática de gerência. O ideal é que apenas os problemas que envolvam um ou alguns poucos usuários ligados a um mesmo equipamento de interconexão sejam descobertos através dos usuários. Se a rede não estiver sendo monitorada, recomendamos que você e sua equipe comecem a planejar o início do monitoramento, para que os problemas possam ser detectados e solucionados mais rapidamente.

Este procedimento, quando necessário, deve ser realizado na fase de coleta de informações (ver Seção 3.2, página 34).

9.3.2 Usando traceroute

Nesta seção veremos como usar `traceroute` para localizar problemas em uma rede.

Para auxiliar o entendimento deste procedimento, vamos apresentá-lo em forma de exemplo. Suponha que alguns usuários informaram que a rede está muito lenta. Este usuários participam do Departamento de Marketing.

Da própria máquina onde você está conectado, você pode direcionar um `traceroute` para uma das máquinas dos usuários ou para o equipamento onde elas estão conectadas. Ao realizar este teste, use sempre endereços IP e nunca nomes de domínio, pois o problema que você quer diagnosticar pode ser no serviço de nomes. Voltando ao exemplo, direcione `traceroute` para a máquina de um usuário. Por exemplo:

```
# traceroute –n 10.16.254.1
1  10.16.75.171  2 ms  1 ms  1 ms
2  10.16.13.97  4 ms  5 ms  4 ms
```

```
3  10.16.24.254  7 ms  8 ms  6 ms
4  10.16.254.33  1936.342 ms  * *
5  10.16.254.1  1959.462 ms  *  1939.310 ms
```

Em redes locais Ethernet não sobrecarregadas (menos de 50% de utilização) os tempos de respostas geralmente não ultrapassam alguns poucos milésimos de segundos. Quando muitos roteadores precisam ser atravessados, é aceitável um atraso maior, mas que não ultrapassa 100 ms. No exemplo acima os tempos de resposta dos equipamentos mostrados nas linhas 4 e 5 são inaceitáveis para uma rede local.

A resposta deste `traceroute` nos mostra que o tempo de resposta do equipamento 4 (10.16.254.33) está inaceitável. Isto não quer dizer que este equipamento em especial está com problema. Esta resposta significa que até o elemento 3 (10.16.24.254) a comunicação está perfeita. As informações obtidas com o resultado do `traceroute` nos ajudam a testar os elementos certos e a focar a nossa atenção onde o problema realmente está ocorrendo.

Se o tempo de resposta de algum dos equipamentos intermediários for mais que 3 segundos ou se o equipamento não responde, serão impressos asteriscos (*) na saída do `traceroute` como mostrado o exemplo a seguir:

O parâmetro –n foi passado para o comando traceroute para indicar que no resultado devem ser apresentados os IPs das máquinas e não seus nomes de domínio.

Na saída do `traceroute` apenas roteadores serão apresentados. Repetidores e comutadores não serão visíveis, portanto. Se a comunicação tornou-se mais lenta ou foi interrompida entre dois equipamentos, e entre eles há repetidores ou comutadores, estes também ficarão sob suspeita.

Com o `traceroute` podemos descobrir o caminho percorrido pelos datagramas até um determinado destino, sendo possível descobrir erros de roteamento na rede facilmente.

Caracteres H! na saída do `traceroute` indicam ausência de rotas. Se você vir estes caracteres após executar o `traceroute` você provavelmente tem um problema de roteamento. Com o resultado você já sabe que equipamento não tem rota apropriada para repassar o datagrama até o destino (alvo do `traceroute`).

No Windows o comando equivalente ao `traceroute` é o `tracert`. Passe o parâmetro –d para que ele não tente mapear IPs em nomes.

Voltemos ao exemplo dos usuários de Marketing. Agora, com o resultado do `traceroute`, você já sabe que realmente existe um problema, e que ele está localizado entre os equipamentos apresentados nas linhas 3 e 4.

9.4 Referências

9.4.1 Recursos online (Internet)

[CISCO-SPAN] Configuring the Catalyst Switched Port Analyzer (SPAN) Feature.

http://www.cisco.com/warp/public/473/41.html

[SNIFFER_PRO-INSTALL] Sniffer Pro Installation Guide.

http://download.nai.com/products/media/sniffer/support/SNP/25/spinstal.pdf

10 Procedimentos referenciados nos problemas de nível físico e enlace

Neste capítulo apresentamos 15 procedimentos que informam como obter e analisar informações de gerência. Os procedimentos apresentados neste capítulo informam como obter os sinais que foram mais referenciados nos problemas de nível físico e de enlace. No entanto, existem alguns problemas de outras camadas que os referenciam.

10.1 Obtendo taxa de erros

Neste procedimento, mostraremos como calcular taxas de erros de entrada e saída e taxas de erros específicas de redes Ethernet com o auxílio de diversas ferramentas de gerência. Na Seção **DESCRIÇÃO E DICAS** definimos taxas de erros de entrada e saída, taxas de erros específicas da tecnologia Ethernet, limiares para cada uma delas e equações que oferecem a taxa de erros de um enlace. Nas seções subseqüentes descrevemos como a taxa de erros pode ser obtida com o auxílio de estações de gerência SNMP, interfaces de linha de comando, analisadores de protocolos e outras ferramentas de gerência.

10.1.1 Descrição e dicas

Erros podem ser detectados durante o recebimento ou a transmissão de um quadro. Desta forma, pode-se definir erros de entrada e erros de saída. A taxa de erros é geralmente expressa como um percentual. Considerando as tecnologias de redes de alta velocidade atuais, as taxas de erros devem estar bastante próximas de `zero`, caso contrário um problema real está ocorrendo [CISCO-PERF-BP].

A taxa de erros de entrada informa o percentual de quadros que chegaram com erros em uma interface e por isso não puderam ser entregues a protocolos de camadas superiores. A taxa de erros de saída é o percentual de quadros que não foram transmitidos devido a erros. A Equação 10.1-1 e a Equação 10.1-2 mostram como calcular as taxas de erros de entrada e saída de um enlace:

$$\text{Taxa de erros de entrada (\%)} = \frac{\text{número de quadros recebidos com erro durante } \Delta T}{\text{número total de quadros recebidos durante } \Delta T} \times 100$$

Equação 10.1-1

$$\text{Taxa de erros de saída (\%)} = \frac{\text{número de quadros não transmitidos devido a erros durante } \Delta T}{\text{Número total de quadros transmitidos durante } \Delta T} \times 100$$

Equação 10.1-2

As equações apresentadas acima são equações gerais, que informam a taxa de erros total de entrada e saída de uma interface no intervalo de tempo ΔT. No entanto, em enlaces Ethernet-like[57], mais comuns em redes locais, vários tipos de erros específicos podem ocorrer. Essas taxas de erros específicos podem ser calculadas separadamente.

Ao perceber uma taxa de erros elevada – uma taxa de erros de entrada de 0,001%, por exemplo – você pode investigar que tipo de erro específico está causando a maior parte dos erros. A Tabela 10-1 apresenta alguns erros de entrada específicos de enlaces Ethernet e a Tabela 10-2 erros de saída.

Tipo de erro	Descrição
Erros de CRC	Quadros com tamanho válido, mas cuja verificação do campo CRC indica que erros de bits ocorreram durante a transmissão. Em enlaces Ethernet de pares trançados espera-se no máximo 1 bit com erro a cada 10^9 bits transmitidos[58] [GUIA-ETHERNET]. Enlaces óticos apresentam transmissão ainda mais precisa, aceitando um máximo de 1 bit com erro a cada 10^{12} bits transmitidos. Na prática o número de erros de bits tipicamente é menor que os descritos acima. Considerando quadros Ethernet grandes (1518 bytes) e enlaces de pares trançados, a taxa de erros CRC máxima apresentada acima poderia ser descrita como 1 erro a cada 82.345 quadros transmitidos. Isto é, uma taxa de erros de no máximo 0,001%. Considerando quadros menores (de 64 bytes) seria possível encontrar no máximo 1 erro a cada 1.953.125 quadros transmitidos, resultando em uma taxa de erros em torno de 0,00005%. Se há preponderância de quadros de tamanho intermediário (727 bytes), pode-se encontrar 1 erro de CRC a cada 171.939 quadros transmitidos, o que oferece uma taxa de erros de aproximadamente 0,0006%. Lembre-se que estes números apresentam os piores casos, e na prática a taxa de erros será tipicamente bem menor que as apresentadas. Taxas de erros de CRC elevadas indicam geralmente problemas na interface remota ou no cabeamento da rede.
Erros de	Quadros que não contêm um número inteiro de octetos (erro de

[57] Enlaces Ethernet, Fast Ethernet, Gigabit Ethernet e 10Gibabit Ethernet.

[58] Na realidade, quanto maior a velocidade do enlace Ethernet mais rigorosos se tornam os objetivos de erros. Para enlaces Gigabit Ethernet, por exemplo, aceita-se 1 bit com erro a cada 10^{12} bits transmitidos.

alinhamento	enquadramento) e que não possuem CRC válido. Um número muito pequeno de erros de alinhamento pode ocorrer com o tempo em um enlace. Portanto, a taxa de erros de alinhamento em um intervalo de tempo também deve ser muito próxima de zero. Se uma interface estiver recebendo muitos quadros com erros de alinhamento, é possível de que a interface ligada a ela ou o cabeamento estejam com problema.
Quadros muito longos	Quadros muito longos (maiores que 1518 bytes) podem ser emitidos quando um computador é ligado ou reiniciado. Portanto, a ocorrência esporádica de quadros longos não indica problema. A ocorrência freqüente de quadros muito longos indica um problema não local, em geral, defeito em *hardware*.
Erros internos da camada MAC	Um quadro não pôde ser recebido devido a um erro interno da camada MAC. O correto é que este tipo de erro não ocorra.

Tabela 10-1: Erros Ethernet de entrada específicos.

Tipo de erro	Descrição
Colisões tardias	Quando uma colisão é detectada e pelo menos um dos quadros envolvidos na colisão já teve mais de 512 bits transmitidos, a colisão deixa de ser uma colisão simples e passa a ser chamada de *colisão tardia*. Ao contrário de colisões simples, colisões tardias são eventos que nunca devem ocorrer em uma rede Ethernet. Elas indicam que um problema sério está ocorrendo na rede (um defeito de *hardware* ou uma rede fora das especificações).
Colisões excessivas	Quadros que não foram transmitidos por terem participado de 16 colisões consecutivas. A ocorrência de colisões excessivas indica um problema na rede. A ocorrência de colisões excessivas nos horários de maior utilização da rede, por exemplo, pode indicar que o meio compartilhado está muitíssimo congestionado e que uma providência urgente deve ser tomada.
Erros internos da camada MAC	Quadros que não foram transmitidos devido a erros internos da camada MAC. A presença constante destes erros sempre é indicativo de problema na interface.
Erros de detecção de portadora	A detecção de portadora falhou ao tentar transmitir um quadro. Este tipo de erro também não deve ocorrer.

Tabela 10-2: Erros Ethernet de saída específicos.

Os erros específicos de entrada podem ocorrer tanto em enlaces *full duplex* quanto em enlaces *half duplex*. No entanto, os erros de saída – com exceção de

erros internos da camada MAC – só são válidos para enlaces operando no modo *half duplex*.

Como já mencionado anteriormente, as taxas de erros de entrada e de saída devem ser números muito próximos de zero. Uma taxa de erros de entrada superior a 0,001% já é alarmante. Quando a taxa de erros de entrada está elevada é mais comum que existam problemas na interface remota, no cabeamento ou interferência os cabos. A taxa de erros de saída deve ser ainda menor que a taxa de erros de entrada. Na realidade ela deve ser 0%, pois a ocorrência de quaisquer dos erros específicos que a compõem indica problema na rede.

Uma outra medida que pode ser tomada como base é a quantidade aceitável de erros em uma hora. Esta medida é freqüentemente mais fácil de obter do que o percentual. Enlaces de pares trançados com vazão média de 1Mbps podem apresentar até no máximo uns 3 erros por hora. Enlaces com vazão média de 6 Mbps já podem apresentar até uns 20 erros por hora. Substituindo v_m pela vazão média do enlace, pode-se aproximar o número máximo aceitável de erros de entrada em uma hora de transmissão através da Equação 10.1-3:

$$\text{Quantidade máxima de erros em uma hora} = \frac{(v_m \times 3600)}{10^9}$$

Equação 10.1-3

10.1.2 Usando uma estação de gerência SNMP

Nesta seção mostraremos como utilizar variáveis SNMP para obter a taxa de erros de um enlace. Serão consideradas taxas de erros de entrada, de saída e específicas da tecnologia Ethernet.

As variáveis **ifInErrors**, **ifInUcastPkts**, **ifInBroadcastPkts** e **ifInMulticastPkts** do Grupo Interfaces da MIB-2 são utilizadas para o cálculo da taxa de erros de entrada. A Equação 10.1-4 pode ser usada para obter a taxa de erros de entrada (ε_{in}) de uma interface.

$$\varepsilon_{in}(\%) \quad \frac{\Delta ifInErrors}{\Delta ifInUcastPkts + \Delta ifInMulticastPkts + \Delta ifInBroadcastPkts + \Delta ifInErrors} \times 100$$

Equação 10.1-4

Onde:

- **ΔifInErrors** é a quantidade quadros que chegaram com erros em uma interface – e por isso não puderam ser entregues ao protocolos da camada superior –durante um certo intervalo de tempo;

- **ΔifInUcastPkts** é a quantidade de quadros com endereços destino *unicast* que chegaram na interface durante um certo intervalo de tempo e foram entregues a protocolos da camada superior;

- **ΔifInBroadcastPkts** é a quantidade de quadros com endereços destino *broadcast* que chegaram na interface durante um certo intervalo de tempo e foram entregues a protocolos da camada superior;

- **ΔifInMulticastPkts** é a quantidade de quadros com endereços destino *multicast* que chegaram na interface durante um certo intervalo de tempo e foram entregues a protocolos da camada superior.

É comum que se use um intervalo de tempo de 5 a 15 minutos entre duas coletas de dados consecutivas. Por exemplo, considere que em um tempo t_0 uma coleta de dados SNMP foi realizada. Neste momento, **$ifInErrors_0$**, **$ifInUcastPkts_0$**, **$ifInBroadcastPkts_0$** e **$ifInMulticastPkts_0$** foram recuperados:

- **$ifInErrors_0$** = 1

- **$ifInUcastPkts_0$** = 2981631

- **$ifInBroadcastPkts_0$**= 2091273

- **$ifInMulticastOkts_0$** = 1012354

Após 5 minutos, em t_1, uma nova coleta foi realizada, recuperando-se novos valores para os contadores **ifInErrors**, **ifInUcastPkts** e **ifInBroadcastPkts** e **ifInMulticastPkts**.

- **$IfInErrors_1$** = 2

- **$IfInUcastPkts_1$** = 4012693

- **$IfInBroadcastPkts_1$** = 2917823

- **$ifInMulticastOkts_0$** = 1519841

Nestes 5 minutos, a taxa de erros de entrada (ε_{in}) da interface em questão é:

$$\varepsilon_{in\%} = \frac{(ifInErrors_1 - ifInErrors_0) \times 100}{ifInUcastPkts_1 - ifInUcastPkts_0 + ifInBroadcastPkts_1 - ifInBroadcastPkts_0 + ifInMulticastPkts_1 - ifInMulticastPkts_0 + ifInErrors_1 - ifInErrors_0}$$

$$\varepsilon_{in\%} = \frac{2 - 1}{(4012693 - 2981631) + (2917823 - 2091273) + (1519841 - 1012354) + (2-1)} \times 100$$

$$\varepsilon_{in\%} = \approx 0{,}00004\%$$

Neste exemplo, a interface em questão recebeu, durante um intervalo de 5 minutos, mais de 2 milhões de quadros e 1 erro ocorreu. Esta é uma taxa de erros aceitável.

Note que, ao utilizar o contador **ifInErrors**, você estará considerando qualquer tipo de erro que impeça o quadro de ser entregue a uma camada superior, incluindo, por exemplo para redes Ether-like, erros de CRC, de enquadramento e recebimento de quadros muito grandes. Cada um destes erros pode ser

calculado individualmente, mas, nestes casos, variáveis de outras MIBs – MIB RMON ou MIBs específicas da tecnologia de transmissão em questão, como MIB Ether-like, por exemplo – deverão ser utilizadas. A taxa de erros específicos deve ser calculada quando for observada uma taxa de erros elevada em uma determinada interface. Neste caso, você pode descobrir que tipo de erro está causando a taxa elevada de erros.

A taxa de erros de saída também pode ser calculada com o auxílio de variáveis do grupo Interfaces da MIB-2: ifOutErrors, ifOutUCastPkts, ifOutMulticastPkts.e ifOutBroadcastPkts. O cálculo é bastante semelhante ao apresentado na Equação 10.1-4:

$$\varepsilon_{in}\,(\%) = \frac{\Delta ifOutErrors}{\Delta ifOutUcastPkts + \Delta ifOutMulticastPkts + \Delta ifOutBroadcastPkts} \times 100$$

Equação 10.1-5

Onde:

- ΔifOutErrors é a quantidade quadros que não puderam ser transmitidos devido a erros durante um certo intervalo de tempo.

- ΔifOutUcastPkts é a quantidade de quadros com endereços destino *unicast* cuja transmissão foi requisitada por protocolos da camada superior durante um certo intervalo de tempo, incluindo quadros descartados ou não enviados.

- ΔifOutBroadcastPkts é a quantidade de quadros com endereços destino *broadcast* cuja transmissão foi requisitada por protocolos da camada superior durante um certo intervalo de tempo, incluindo quadros descartados ou não enviados.

- ΔifOutMulticastPkts é a quantidade de quadros com endereços destino *multicast* cuja transmissão foi requisitada por protocolos da camada superior durante um certo intervalo de tempo, incluindo quadros descartados ou não enviados.

Nas próximas sub-seções serão apresentadas equações que devem ser utilizadas para o cálculo de vários tipos de erros específicos de entrada e de saída em redes Ether-like. Em todas elas, variáveis do tipo contador são utilizadas. Estas variáveis são precedidas sempre do símbolo Δ para que você se lembre que o valor do incremento desta variável em um determinado intervalo de tempo é que deve ser utilizado em cada equação.

10.1.2.1 TAXA DE ERROS DE CRC

Os erros de CRC são considerados erros de entrada. Quando um quadro chega com erro de CRC significa que pelo menos um bit do quadro foi alterado durante a transmissão. A taxa de erros de CRC pode ser calculada utilizando-se a

variável **dot3StatsFCSErrors** da MIB Ether-Like [RFC2665] e as variáveis **ifInUcastPkts**, e **ifInBroadcastPkts** e **ifInMulticastPkts** do Grupo Interfaces da MIB-2 [RFC2233]. Veja a Equação 10.1-6.

$$\text{Taxa de Erros de CRC (\%)} = \frac{\Delta\,\text{dot3StatsFCSErrors x 100}}{\Delta\text{ifInUcastPkts} + \Delta\text{ifInMulticastPkts} + \Delta\text{ifInBroadcastPkts} + \Delta\text{dot3StatsFCSErrors}}$$

Equação 10.1-6

Onde:

- **ΔetherStatsFCSErrors** é a quantidade de quadros recebidos com erro de CRC pela interface em um determinado período de tempo.

10.1.2.2 TAXA DE ERROS DE ALINHAMENTO

A taxa de erros de alinhamento pode ser calculada utilizando-se a variável **dot3StatsAlignmentErrors** da MIB Ether-Like [RFC2665] e as variáveis **ifInUcastPkts**, **ifInBroadcastPkts** e **ifInMulticastPkts** do grupo Interfaces da MIB-2 [RFC2233]. A Equação 10.1-7 informa como calcular a taxa de erros de alinhamento.

$$\text{Taxa de Erros de Alinhamento (\%)} = \frac{\Delta\,\text{dot3StatsAlignmentErrors}}{\Delta\text{ifInUcastPkts} + \Delta\text{ifInMulticastPkts} + \Delta\text{ifInBroadcastPkts} + \Delta\text{ifInErrors}} \text{ x 100}$$

Equação 10.1-7

Onde:

- **ΔetherStatsAlignmentErrors** é a quantidade de quadros recebidos com erro de alinhamento pela interface em um determinado período de tempo.

A MIB RMON [RFC1757] não traz contadores para erros de CRC e alinhamento separadamente. O contador **etherStatsCRCAlignErrors** é incrementado sempre que um quadro com erro de CRC ou de alinhamento for recebido. Com o auxílio desta variável de gerência e da variável **etherStatsPkts** é possível calcular a taxa de erros de CRC e alinhamento de uma interface seguindo a Equação 10.1-8.

$$\text{Taxa de Erros de CRC e alinhamento (\%)} = \frac{\Delta\text{etherStatsCRCAlignErrors}}{\Delta\text{etherStatsPkts}} \text{ x 100}$$

Equação 10.1-8

Onde:

- **ΔetherStatsCRCAlignErrors** é a quantidade de quadros com erro de CRC ou erro alinhamento recebido pela interface em um determinado intervalo de tempo.

- **ΔetherStatPkts** é a quantidade total de pacotes recebidos, incluindo quadros com erro, e quadros destinados a endereços *broadcast* e *multicast* em um determinado intervalo de tempo.

10.1.2.3 TAXA DE ERROS INTERNOS DE RECEPÇÃO DA CAMADA MAC

Em interfaces Ethernet, outros erros além de erros de CRC, alinhamento ou quadros muito grandes podem impedir que um quadro seja transmitido para camadas superiores (erro de entrada). Quando isto ocorrer, o contador **dot3StatsInternalMacReceiveErrors** da MIB Ether-Like será incrementado. Assim, você pode calcular a taxa de erros internos da camada MAC como mostrado na Equação 10.1-9:

$$\text{Taxa de erros internos de recepção (\%)} = \frac{\Delta dot3StatsInternalMacReceiveErrors \times 100}{\Delta ifInUcastPkts + \Delta ifInMulticastPkts + \Delta ifInBroadcastPkts + \Delta dot3StatsInternalMacReceiveErrors}$$

Equação 10.1-9

Onde:

- **Δdot3StatsInternalMacReceiveErrors** é a quantidade de quadros que não foram entregues a protocolos da camada superior devido a erros internos na sub-camada MAC em um determinado período de tempo.

No procedimento apresentado na Seção 10.11 será visto como obter a quantidade de quadros muito longos recebidos por um enlace.

10.1.2.4 TAXA DE COLISÕES EXCESSIVAS

Objetos das MIBs Ether-like e do grupo Interfaces serão utilizados. O objeto **dot3StatsExcessiveCollisions** é incrementado sempre que um quadro não for transmitido por ter sofrido 16 colisões consecutivas. A Equação 10.1-10 pode ser utilizada no cálculo da taxa de ocorrência de colisões excessivas:

$$\text{Taxa de colisões excessivas (\%)} = \frac{\Delta dot3StatsExcessiveCollisions}{\Delta ifOutUcastPkts + \Delta ifOutMulticastPkts + \Delta ifOutBroadcastPkts} \times 100$$

Equação 10.1-10

Onde:

- **Δdot3StatsExcessiveCollisions** é a quantidade de colisões excessivas ocorridas em um determinado intervalo de tempo.

10.1.2.5 TAXA DE ERROS INTERNOS DE TRANSMISSÃO DA CAMADA MAC

O contador dot3StatsMacTransmitErrors é incrementado sempre que um quadro não pode ser transmitido devido a um erro que não se enquadra em nenhum dos demais erros específicos de transmissão (colisão tardia, colisões excessivas ou falha na detecção da portadora). A taxa de erros internos de transmissão pode ser obtido através da Equação 10.1-11.

$$\text{Taxa de Erros Internos de transmissão (\%)} = \frac{\Delta \text{dot3StatsInternalMacTransmitErrors}}{\Delta \text{ifOutUcastPkts} + \Delta \text{ifOutMulticastPkts} + \Delta \text{ifOutBroadcastPkts}} \times 100$$

Equação 10.1-11

Onde:

- ∆dot3StatsInternalMacTransmitErrors é a quantidade de quadros que não foram transmitidos devido a erros internos na sub-camada MAC em um determinado período de tempo.

O **VERIFICANDO OCORRÊNCIA DE COLISÕES TARDIAS** informa como verificar se colisões tardias estão ocorrendo na rede.

10.1.3 Usando um analisador de protocolos

Nesta seção mostraremos como podemos verificar a ocorrência de erros em um enlace com o auxílio de um analisador de protocolos.

O primeiro passo é conectar o analisador corretamente, como descrito no UTILIZANDO UM ANALISADOR DE PROTOCOLOS. Infelizmente, a função de espelhamento não poderá ser utilizada quando desejamos ver erros físicos de um enlace, pois os quadros com erros não são repassados para a porta na qual os dados estão sendo espelhados [CISCO-SPAN]. Você terá que usar um repetidor auxiliar ou um *splitter*.

Seguindo as dicas deste mesmo procedimento (página 226), verifique no painel do Sniffer e no painel de detalhes os erros que estão ocorrendo. Se os contadores de erros estiverem crescendo continuamente, existe algum problema.

Você também pode utilizar a funcionalidade de amostragem histórica. O Sniffer pode criar para você gráficos de erros/s. É interessante criar um gráfico com estatísticas múltiplas que mostre quantidade de erros e octetos por segundo. Dicas para a utilização desta funcionalidade do Sniffer podem ser encontradas na Seção OUTRAS FUNÇÕES INTERESSANTES DO SNIFFER (página 226).

10.1.4 Usando interface de linha de comando

Nesta seção mostramos comandos da interface de linha de comando de roteadores e comutadores Cisco que oferecem informações sobre erros nos enlaces.

O *software* de todos os comutadores e roteadores oferece comandos que apresentam estatísticas das interfaces do equipamento. Na maioria dos roteadores Cisco o seguinte comando pode ser executado:

```
roteador# show interface <tipo da interface> <número da interface>
```

Para analisar estatísticas da porta Fast Ethernet 1/0/0 de um roteador Cisco use o comando a seguir:

```
roteador# show interface FastEthernet 1/0/0
1.  FastEthernet1/0/0 is up, line protocol is up
2.  Hardware is cyBus FastEthernet Interface, address is
    0002.1743.9820 (bia 0002.1743.9820)
3.  Internet address is 208.145.167.233/24
4.  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load
    8/255
5.  Encapsulation ARPA, loopback not set
6.  Keepalive set (10 sec)
7.  Half-duplex, 100Mb/s, 100BaseTX/FX
8.  ARP type: ARPA, ARP Timeout 04:00:00
9.  Last input 00:00:00, output 00:00:00, output hang never
10. Last clearing of "show interface" counters never
11. Queueing strategy: fifo
12. Output queue 0/40, 0 drops; input queue 0/75, 0 drops
13. 5 minute input rate 572000 bits/sec, 462 packets/sec
14. 5 minute output rate 3527000 bits/sec, 563 packets/sec
15.     484455791 packets input, 2990640235 bytes, 0 no buffer
16.     Received 344792 broadcasts, 0 runts, 0 giants, 0 throttles
17.     1 input errors, 1 CRC, 0 frame, 0 overrun, 0 ignored
18.     0 watchdog, 0 multicast
19.     0 input packets with dribble condition detected
20.     520096751 packets output, 3410608492 bytes, 0 underruns
21.     1 output errors, 5373084 collisions, 3 interface resets
22.     0 babbles, 1 late collision, 0 deferred.
23.     0 lost carrier, 0 no carrier
24.     0 output buffer failures, 0 output buffers swapped out
```

As linhas 16 e 17 mostram contadores de erros de entrada e as linhas 20 e 21 contadores de erros de saída. Nas linhas 15 e 20 são apresentados, respectivamente, contadores de pacotes que entraram e foram transmitidos pela interface.

Em comutadores Cisco use o comando:

```
console> show port [[módulo]/porta]
```

Ele apresentará, dentre outras informações, contadores de erros de uma interface. Por exemplo, use o comando a seguir para verificar estatísticas da porta 1/1 de um comutador:

```
Console> show port 1/1

Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 1/1                     connect    1            auto  auto 10/100BaseTX

(…)

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          1          1          1         0

Port Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts  Giants
---- ---------- ---------- ---------- ---------- --------- ------ -------
 1/1          0          0          0          1         0      0       0

Last-Time-Cleared
--------------------------
Wed Jan 20 2002, 13:03:12
```

O comando a seguir oferece contadores de erros para todas as portas do comutador:

```
comutador> show port counters
```

Infelizmente este comando não apresenta contadores de quadros de entrada e saída, mas eles podem ser obtidos através do comando a seguir:

```
comutador> show port mac [[módulo]/porta]
```

Além deste comando, alguns comutadores Cisco oferecem o comando `show counters`, que gera uma cópia dos contadores do comutador, incluindo a quantidade de pacotes recebidos por uma interface e a quantidade de pacotes que chegaram com erros.

O mesmo cálculo realizado anteriormente, ao apresentar como se calcula a taxa de erros com o auxílio de uma estação de gerência SNMP é válido aqui. Analisar o resultado de uma única execução destes comandos não faz sentido, pois eles retornam valores de contadores cumulativos. Portanto, uma análise só faz sentido se você obtiver o valor do contador desejado e após um certo intervalo de tempo recuperá-lo novamente. Desta forma, você poderá calcular a taxa de erros. O cálculo é idêntico ao realizado utilizando uma estação de gerência SNMP.

10.1.5 Usando ifconfig e netstat

Nesta secção apresentamos ferramentas de gerência que oferecem informações sobre erros em interfaces de hospedeiros.

O comando `ifconfig` do Linux/Unix também pode ser utilizado para recuperar a taxa de erros de uma interface. Ao passar para este comando o argumento `–a`, são apresentadas estatísticas de todas as interfaces da máquina, incluindo um contador de erros e um contador de pacotes recebidos. O mesmo procedimento apresentado nas seções anteriores (como calcular taxa de erros com o auxílio de interfaces de linhas de comando) são válidos: recupere os valores dos contadores de erros e pacotes recebidos ou transmitidos em dois intervalos de tempos distintos (t_0 e t_1, por exemplo) e em seguida substitua os valores encontrados na Equação 10.1-1 ou na Equação 10.1-2. Veja a seguir um exemplo da execução do comando `ifconfig`. Em negrito estão as informações que você irá utilizar para o cálculo das taxas de erros de entrada e saída.

```
[maria@server ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:04:AC:4C:98:DF
          inet addr:102.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10626336 errors:3 dropped:0 overruns:0 frame:0
          TX packets:9429316 errors:1 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2471067525 (2356.5 Mb)  TX bytes:1160820381 (1107.0 Mb)
          Interrupt:15 Base address:0x2180

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:926558 errors:0 dropped:0 overruns:0 frame:0
          TX packets:926558 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:129180878 (123.1 Mb)  TX bytes:129180878 (123.1 Mb)
```

Se preferir pode utilizar também o seguinte comando, que oferece praticamente as mesmas informações do comando anterior:

```
[maria@server ~]$ netstat -i
Kernel Interface table
Iface  MTU Met  RX-OK    RX-ERR  RX-DRP  RX-OVR  TX-OK   TX-ERR  TX-DRP  TX-OVR  Flg
eth0   1500     1062665  3       0       0       942960  1       0       0       BMRU
lo     16436    0        926584  0       0       0       926584  0       0       LRU
```

Em máquinas Windows use o comando `netstat –ne` para recuperar quantidade de quadros transmitidos e recebidos e erros detectados:

```
C:\WINDOWS>netstat -ne
Estatísticas de interface
                            Recebido  Enviado
Bytes                       242119    30360
Pacotes unicast             516       451
```

Pacotes não unicast	24	32
Descartados	1	1
Erros	2	0
Prot. Desconhecidos	23	

Para calcular a taxa de erros de entrada substitua os valores obtidos com este comando na Equação 10.1-1 e Equação 10.1-2.

10.2 Obtendo a taxa de colisões

Neste procedimento falaremos sobre taxa de colisões. Na Seção **DESCRIÇÃO E DICAS** discutiremos que taxa de colisões devemos considerar elevadas. Nas seções seguintes você aprenderá como calcular taxas de colisões de enlaces Ethernet com o auxílio de uma estação de gerência SNMP, de um analisador de protocolos, de uma interface de linha de comandos e de outras ferramentas de gerência.

10.2.1 Descrição e Dicas

Colisões são ocorrências normais em meios Ethernet compartilhados (*half duplex*[59]). Uma taxa elevada de colisões – maior que a habitual – no entanto, pode ser um indicativo de problema. Alguns problemas que causam o aumento da taxa de colisões em um enlace são: domínio de colisões congestionado, descasamento de modo de transmissão e *hardware* defeituoso.

Alguns administradores de redes acreditam que não mais de 1% dos quadros transmitidos devem colidir; outros acreditam que só a partir de 20% de taxa de colisões devemos nos preocupar. Nós fazemos parte de uma turma menos extremista: 10% é a taxa máxima de colisões que aceitamos. Em [PERF&FAULT-CISCO] encontramos uma análise bastante interessante sobre colisões. A seguir veremos um resumo desta análise.

Uma taxa de colisões até 10% não causará problemas à rede. As colisões são detectadas pela própria camada de enlace, e a retransmissão dos quadros que colidiram é de sua responsabilidade. Assim, a retransmissão é praticamente instantânea. Por isso, taxas de colisões até 10% não degradam o desempenho da rede. O mesmo não ocorre com colisões tardias, erros de CRC ou quadros muito grandes. O limiar para estas taxas deve ser bem menor, uma vez que a retransmissão destes quadros só é feita após um certo timeout de camadas superiores. Isto sim, degrada substancialmente o desempenho da rede e pode irritar os usuários.

Conclusão: é importante estar de olho nas taxas de colisões de enlaces – pelo menos os mais críticos. No entanto, é ainda mais importante verificar a ocorrência de erros como CRC, alinhamento, quadros muito grandes e colisões

[59] Em ambientes *full duplex* a taxa de colisões deve ser zero.

tardias. Uma taxa de 0.1% de erros de CRC degrada muito mais o desempenho da rede que uma taxa de 10% de colisões.

A taxa de colisões aumenta quando aumenta a utilização do enlace half duplex. A Tabela 10-3 [PERF&FAULT-CISCO] dá uma idéia de como a taxa de colisões aumenta em função do aumento da utilização do enlace.

Utilização do segmento	Percentual de pacotes que colidem
0 – 19%	1%
20 – 49%	5%
> 50%	15%

Tabela 10-3: Taxas de colisões versus utilização

Geralmente, a Equação 10.2-1 pode ser utilizada para obter a taxa de colisões de um enlace.

$$\text{Taxa de colisões (\%)} = \frac{\text{Quantidade de quadros que colidiram durante } \Delta T}{\text{Quantidade de quadros transmitidos durante } \Delta T} \times 100$$

Equação 10.2-1

De acordo com esta equação, a taxa de colisões é o percentual de quadros que colidiram com relação à quantidade total de quadros transmitidos (incluindo quadros que colidiram). Comutadores e estações de trabalho só conseguem detectar as colisões nas quais se envolvem (chamadas por alguns fabricantes de colisões locais). Por esta razão, não estamos considerando a quantidade de quadros recebidos pela interface na equação.

Em situações em que todas as colisões, inclusive as remotas, são detectadas (isso pode ser o caso em algumas sondas RMON), a equação da taxa de colisões será um pouco diferente. Ela considerará todo o tráfego de entrada e saída. Veja a Equação 10.2-2.

$$\text{Taxa de colisões (\%)} = \frac{\text{Quantidade de quadros que colidiram durante } \Delta T}{\text{Quantidade de quadros transmitidos e recebidos durante } \Delta T} \times 100$$

Equação 10.2-2

O intervalo ΔT pode variar entre 1 minuto e 1 hora. Aconselhamos que este intervalo não ultrapasse 5 minutos quando equipamentos críticos (de *backbone*, por exemplo) estiverem envolvidos.

10.2.2 Usando uma Estação de Gerência SNMP

Nesta seção apresentaremos os objetos SNMP que podem ser combinados para calcular a taxa de colisões de um enlace Ethernet *half duplex*.

Os seguintes objetos auxiliarão no cálculo da taxa de colisões:

- dot3StatsSingleCollisionFrames e dot3StatsMultipleCollisionFrames da MIB Ether-Like [RFC2358], que contam, respectivamente, a quantidade de quadros que colidiram uma única vez ou múltiplas vezes antes que a transmissão fosse possível;

- etherStatsCollisions da MIB RMON [RFC1757], que informa o número total de colisões em um segmento (simples e múltiplas).

A taxa de colisões de uma interface pode ser calculada como apresentado na Equação 10.2-3:

$$\text{Taxa de colisões (\%)} = \frac{\Delta\text{dot3StatsSingleCollisionFrames} + \Delta\text{dot3StatsMultipleCollisionFrames}}{\Delta\text{ifOutUcastPkts} + \Delta\text{ifOutBroadcastPkts} + \Delta\text{ifOutMulticastPkts}} \times 100$$

Equação 10.2-3

Onde:

- ∆dot3StatsSingleCollisionFrames é a quantidade de colisões simples que ocorreram em um determinado intervalo de tempo;

- ∆dot3StatsMultipleCollisionFrames é a quantidade de colisões múltiplas detectadas por uma interface durante um determinado intervalo de tempo.

Para uma definição de ∆ifOutUcastPkts, ∆ifOutBroadcastPkts e ∆ifInMulticastPkts veja Seção 10.1.2. O somatório das 3 variáveis fornece o total de quadros de saída na interface em questão.

Lembrete: todas as variáveis utilizadas nos cálculos apresentados são do tipo contador. Portanto, apenas a variação destes contadores no tempo faz sentido. O valor puro do contador não nos diz se houve ou não muitas colisões. Mas se obtemos o valor do incremento do contador no tempo podemos ter uma idéia de sua taxa de crescimento. Por exemplo, se foram realizadas coletas de dados SNMP em t_0 e t_1, então:

$$\Delta\text{dot3StatsSingleCollisionFrames} = \text{dot3StatsSingleCollisionFrames}_1 - \text{dot3StatsSingleCollisionFrames}_0.$$

Podemos também calcular a taxa de colisões de um enlace com objetos do grupo de estatísticas da MIB RMON [RFC 1757]. O objeto etherStatsCollisions é uma estimativa do número total de colisões ocorridas no segmento. Veja Equação 10.2-4.

$$\text{Taxa de colisões (\%)} = \frac{\Delta\text{etherStatCollisions}}{\Delta\text{ifOutUcastPkts} + \Delta\text{ifOutBroadcastPkts} + \Delta\text{ifOutMulticastPkts}} \times 100$$

Equação 10.2-4

A Equação 10.2-1 é a mais utilizada no cálculo da taxa de colisões. No entanto, como já comentamos na Seção **DESCRIÇÃO E DICAS**, podem existir situações em que a equação da taxa de colisões é um pouco diferente. Por exemplo, quando um equipamento detecta colisões remotas, isto é, colisões das quais não

participa devemos considerar no cálculo da taxa de colisões não apenas a quantidade de quadros transmitidos, mas também a quantidade de quadros recebidos (Equação 10.2-2).

Repetidores 10Base-2 e 10Base-5 com uma sonda RMON embutida podem detectar colisões remotas. Sendo este o seu caso, a equação Equação 10.2-5 a seguir pode ser usada.

$$\text{Taxa de colisões (\%)} = \frac{\Delta \text{etherStatsCollisions}}{\Delta \text{etherStatsPkts} + \Delta \text{etherStatsCollision}} \times 100$$

Equação 10.2-5

Esta equação também pode ser usada se você tiver uma única máquina ligada a uma porta de um comutador operando em modo *half duplex*. Mas, neste caso aconselhamos que você configure o comutador e a máquina (se for o caso) para trabalharem em modo *full duplex*, eliminando assim colisões, em vez de ficar se preocupando com a taxa de colisões deste enlace.

Se você possui uma sonda RMON monitorando um enlace Ethernet com taxa de colisões elevada e utilização de enlaces também elevada, você pode configurar a sonda para reportar, por exemplo, quais são as 10 máquinas que mais transmitem dados na rede em 15 minutos. Com essa informação, você poderá investigar se esses maiores transmissores estão com defeito de *hardware*, e por isso estão gerando tanto tráfego. Use o grupo hostTopN. A configuração da sonda RMON seria a apresentada na Tabela 10-4. Com esta configuração, a sonda RMON apresentará os 10 maiores transmissores de quadros no segmento de rede sendo monitorado.

hostTopNRateBase	hostTopNOutPkts (2)
hostTopNTimeRemaining	900 segundos (15 minutos)
hostTopNRequestedSize	10

Tabela 10-4: Configuração de hostTopN para obter 10 maiores transmissores em 15 minutos.

10.2.3 Usando um analisador de protocolos

Nesta seção veremos como obter a taxa de colisões a partir de um analisador de protocolos e como ele pode ajudar a encontrar as estações que mais se envolvem em colisões ao tentar transmitir dados.

Conecte o analisador de protocolos conforme descrito no UTILIZANDO UM ANALISADOR DE PROTOCOLOS (página 217). Infelizmente, para que o analisador veja as colisões ocorridas você não poderá usar a função de espelhamento, tendo que conectar o analisador com o auxílio de um repetidor ou *splitter*.

Seguindo ainda as dicas deste mesmo procedimento (página 226), verifique no painel do Sniffer e no painel de detalhes os contadores de colisões. Veja o

incremento dos contadores de quadros e de colisões durante um intervalo de tempo ΔT. Em seguida, use a Equação 10.2-2 para encontrar a taxa de colisões do domínio.

Você também pode utilizar a funcionalidade de amostragem histórica. O Sniffer pode criar para você gráficos de colisões/s. É interessante criar um gráfico com estatísticas múltiplas que mostre quantidade de colisões/s e quadros/s. Dicas para a utilização desta funcionalidade do Sniffer podem ser encontradas na Seção OUTRAS FUNÇÕES INTERESSANTES DO SNIFFER (página 226).

Se você verificar uma taxa elevada de colisões, é interessante tentar descobrir se existe uma estação que se envolve mais em colisões que as demais estações. A análise descrita a seguir, descrita em [HAUGDAHL], pode ser interessante, especialmente quando se desconfia de problemas de hardware ou cabeamento.

No Sniffer existe o filtro **Default**, que permite que todos os quadros sejam capturados. Escolha este filtro e inicie a captura. Observe na tela de detalhamento de estatísticas Ethernet se durante a captura colisões ocorreram. Após algumas dezenas de colisões terem ocorrido, finalize a captura

O preâmbulo dos quadros Ethernet não é mostrado pelos analisadores. Mas quando dois preâmbulos colidem e geram uma seqüência de dois 1s seguidos, o analisador começa a receber um quadro prematuramente. Todo o restante do preâmbulo ainda é enviado. Então os dados do preâmbulo são apresentados pelo analisador como se fossem parte do cabeçalho do quadro Ethernet.

O preâmbulo é formado por uma seqüência de 1s e 0s: 10101010… Em hexadecimal esta seqüência forma o padrão AAA… Quando quadros colidem a seqüência do preâmbulo pode se tornar (em hexadecimal) uma seqüência de 555…, pois em binário essa seqüência é formada por 0101…, ou uma seqüência de As e 5s. Ao decodificar os quadros no analisador podemos perceber esses padrões.

Agora lembre-se que: ao detectar uma colisão, uma estação tentará retransmitir o seu quadro que colidiu rapidamente. Isto garante que você verá na tela de decodificação do analisador após a colisão pelo menos dois quadros (os que participaram da colisão). Observando os próximos 2 ou 3 quadros após a colisão temos certeza que pelo menos 2 deles participaram da colisão. Após analisar várias colisões pode-se chegar à conclusão que uma estação está quase sempre envolvida nas colisões.

Se você percebeu que os quadros transmitidos pela estação A quase sempre colidem, monitore a taxa de colisões no enlace ao mesmo tempo que força a máquina A a transmitir mais dados. Por exemplo, faça uma transferência de arquivos da máquina A para outra. Se a taxa de colisões do enlace aumentar bastante durante a transferência dos dados, certamente há algo errado com a placa de rede da estação A ou seu cabeamento.

10.2.4 Usando uma interface de linha de comando

Nesta seção apresentaremos alguns comandos que podem ser executados em roteadores e comutadores e que oferecem os dados necessários para o cálculo da taxa de colisões. Como em todos os outros procedimentos, equipamentos Cisco serão utilizados como exemplo. Se você possui equipamentos de outros fabricantes, procure no manual do seu equipamento quais os comandos que lhe oferecem contadores de colisões detectadas e quadros transmitidos.

Em roteadores Cisco com IOS versão 10.0 ou superior, execute o seguinte comando:

```
roteador# show interfaces <tipo da interface> <número da interface>
```

Este comando apresenta estatísticas da interface escolhida. Veja o resultado deste comando em um roteador Cisco 7507:

```
roteador>show inter fast 1/0/0
FastEthernet1/0/0 is up, line protocol is up
  Hardware is cyBus FastEthernet Interface, address is 0002.1743.9820 (bia
0002.1743.9820)
  Internet address is 200.129.64.139/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 12/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 3064000 bits/sec, 931 packets/sec
  5 minute output rate 5078000 bits/sec, 1002 packets/sec
     245369996 packets input, 3191315201 bytes, 0 no buffer
     Received 54142 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     262296267 packets output, 653636588 bytes, 0 underruns
     1 output errors, 12453993 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Os dados em destaque (negrito) podem ser utilizados para o cálculo da taxa de colisões do enlace. Obtenha a variação destes contadores em um intervalo de tempo ΔT e substitua os valores na Equação 10.2-1.

Em comutadores Cisco o seguinte comando apresenta, dentre outras informações, um contador de colisões:

```
console> show port [módulo[/porta]]
```

Para recuperar valores de contadores de quadros transmitidos e recebidos execute o seguinte comando:

```
console> show mac [módulo[/porta]]
```

Além destes, o comando abaixo também pode ser utilizado.

```
console> show counters
```

Este comando apresenta valores de contadores da porta, incluindo quantidade de colisões detectadas e de quadros transmitidos. Recupere a variação do contador de colisões e de quadros transmitidos durante um determinado intervalo de tempo e substitua os valores na Equação 10.2-1 para obter a taxa de colisões de uma interface.

10.2.5 Usando ifconfig

Esta seção apresenta como obter os dados necessários para o cálculo da taxa de colisões a partir de uma estação Linux.

O comando `ifconfig` pode ser utilizado para recuperar contadores de quadros transmitidos e colisões. Recupere estes contadores com o comando:

```
# ifconfig –a <interface>
```

Veja um exemplo da execução deste comando:

```
# ifconfig –a eth0
eth0 Link encap:Ethernet  HWaddr 00:60:94:63:6E:3A
     inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:658685 errors:0 dropped:0 overruns:0 frame:3
     TX packets:555222 errors:0 dropped:0 overruns:19 carrier:1
     collisions:44644 txqueuelen:100
     Interrupt:5
```

Em destaque estão os dados que você precisa para calcular a taxa de colisões da interface eth0. Lembre-se que estes dados são contadores. Recupere a variação destes contadores durante um determinado intervalo de tempo e substitua os valores obtidos na Equação 10.2-1.

10.3 Verificando ocorrência de colisões tardias

Neste procedimento descrevemos como verificar se colisões tardias estão ocorrendo na rede.

10.3.1 Descrição e dicas

Colisões (sejam elas tardias ou não) só são detectadas por interfaces que estão operando no modo *half duplex*. Portanto, tudo que se falar aqui só é válido para enlaces Ethernet *half duplex*, nos quais o protocolo CSMA/CD é utilizado.

Antes de transmitir qualquer dado, uma estação verifica se o meio está ou não livre e só transmite seus dados quando ela acha que o meio está disponível. No entanto, duas ou mais estações podem simultaneamente (dentro de uma pequena janela de tempo) verificar que o meio está livre e, também simultaneamente, podem começar a transmitir seus dados. O resultado disso é uma colisão.

Uma colisão sempre deve ser detectada antes que os primeiros 512 bits dos quadros envolvidos na colisão tenham sido transmitidos. Quando a colisão é detectada e mais de 512 bits de pelo menos um quadro envolvido já tiverem sido transmitidos, ela passa a ser chamada de colisão tardia.

Colisões tardias nunca devem ocorrer. Sua ocorrência é sinal de que a rede tem problemas de projeto (não seguiu as regras de cabeamento de forma correta), existe alguma interface de equipamento com defeito ou ainda existe descasamento de modo de operação.

10.3.2 Usando uma estação de gerência SNMP

Apresentaremos nesta seção os objetos SNMP que informam a quantidade de colisões tardias que ocorrem em um enlace. Além disso daremos dicas de como configurar alarmes para colisões tardias em uma sonda RMON.

Observe o valor do contador dot3StatsLateCollisions da MIB Ether-Like [RFC2665]. Ele é incrementado sempre que uma colisão tardia é detectada. Portanto, o correto é que ele jamais seja alterado. Se seu valor for incrementado, uma colisão tardia foi detectada e, portanto, você tem algum problema na rede.

Se você tem uma sonda RMON monitorando um enlace *half duplex*, pode configurar um alarme que é disparado quando o contador dot3StatsLateCollisions da interface em questão for incrementado. Na Tabela 10-5 são apresentados alguns dados do alarme a ser configurado na sonda RMON.

Variável a ser monitorada:	dot3StatsLateCollisions
Tipo:	DeltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	1
Limiar decrescente:	0

Tabela 10-5: Dados para configuração de alarme para ocorrência de colisões tardias.

O alarme deve gerar uma notificação (*trap*) para a estação de gerência apenas quando o limiar crescente for atingido.

10.3.3 Usando uma interface de linha de comando

Informaremos nesta seção que comandos em roteadores/comutadores Cisco informam a quantidade de colisões tardias em um enlace. Os comandos apresentados aqui servem para a maioria dos roteadores e comutadores Cisco. Se você possui um equipamento produzido por outro fabricante pesquise no manual do seu equipamento que comando utilizar. É bastante provável que exista um comando semelhante aos apresentados a seguir que lhe dê estatísticas de interfaces.

Em roteadores Cisco com IOS 10.0 ou superior execute o comando a seguir:

```
roteador# show interface <tipo> <número>
```

Por exemplo:

```
roteador# show inter FastEthernet 1/0/0
FastEthernet1/0/0 is up, line protocol is up
Hardware is cyBus FastEthernet Interface, address is 0003.2853.0931 (bia 0003.2853.0931)
Internet address is 192.168.4.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 10/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 98 drops; input queue 0/75, 0 drops
  5 minute input rate 901000 bits/sec, 566 packets/sec
  5 minute output rate 4104000 bits/sec, 678 packets/sec
     2159137620 packets input, 346328816 bytes, 0 no buffer
     Received 1026648 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 4 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1784610 packets output, 142194201 bytes, 0 underruns
     1664 output errors, 48521009 collisions, 11 interface resets
     0 babbles, 1 late collision, 0 deferred
     1663 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out0
```

Neste exemplo, o contador de colisões tardias está com o valor 1 (linha 22). Com este valor único não podemos concluir que a rede está com problemas no momento. Este contador pode ter sido incrementado no passado, indicando um

problema que já foi solucionado. Guarde este valor e mais tarde veja se o contador foi ou não incrementado. Se após alguns minutos, por exemplo, o contador tiver sido incrementado, existe algum problema sério na rede.

Na maioria dos comutadores Cisco execute o comando:

```
console> show port [módulo [/porta]]
```

Este comando apresenta várias estatísticas de uma porta ou de todas as portas de um módulo. Dentre estas estatísticas encontra-se um contador de colisões tardias. Por exemplo, para analisar as informações da porta 1 do módulo 1 de um comutador execute o seguinte comando:

```
Console> show port 1/1

Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 1/1                     connect    1            auto  auto 10/100BaseTX

(…)

Port Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts  Giants
---- ---------- ---------- ---------- ---------- --------- ------ -------
 1/1          0          0          1          0         0      0       0

Last-Time-Cleared
--------------------------
Wed Jan 20 2002, 13:03:12
```

10.4 Obtendo estado operacional de equipamentos

Neste procedimento serão apresentadas algumas formas de se obter o estado operacional de um equipamento.

10.4.1 Descrição e dicas

O estado operacional de um equipamento nos informa se o equipamento está ou não em operação. Equipamentos podem se tornar não operacionais devido a falhas no sistema de alimentação de energia ou devido a defeitos.

Existe um fato que facilita a obtenção do estado operacional de um equipamento: o equipamento não operacional não responderá a qualquer requisição SNMP ou qualquer outra tentativa de comunicação. Então, qualquer que seja a instrumentação utilizada, se não conseguimos qualquer comunicação com o equipamento alvo podemos concluir que ele não está operacional.

10.4.2 Usando uma estação de gerência SNMP

Nesta seção descrevemos como obter o estado operacional de um equipamento utilizando uma estação de gerência SNMP.

De tempos em tempos, a estação de gerência se comunica com os agentes instalados nos dispositivos de rede em busca de dados de gerência SNMP. Se uma estação de gerência não obtiver resposta alguma do agente em um dado momento, ela considera que o dispositivo pelo qual o agente responde não está

operacional. Na realidade, não se pode concluir com certeza se é o dispositivo que está não operacional ou se a comunicação com ele, por alguma razão, não está sendo possível. Dentre as razões que podem deixar a estação de gerência e um equipamento incomunicáveis encontram-se enlaces de comunicação com problema e congestionamento momentâneo da rede.

Não existe uma variável de gerência que indica se o equipamento está ou não em operação. Se existisse, o valor desta variável só poderia ser recuperado quando o dispositivo estivesse em funcionamento. O próprio comportamento do dispositivo, de responder ou não consultas SNMP, nos informa se o equipamento está ou não operacional. Assim, a consulta a qualquer variável pode ser usada para a obtenção do estado operacional de um dispositivo.

Aconselhamos que a variável utilizada para a obtenção do estado operacional do equipamento seja sysUpTime, da MIB-2 [RFC1213]. Esta variável informa a quantidade de tempo, em centésimos de segundos, que se passou desde a última vez que o equipamento foi reiniciado. Se em um determinado momento o valor desta variável é menor que o seu valor na última coleta SNMP, significa que o equipamento foi reiniciado ou que ele passou mais que 497 dias em operação. O valor máximo desta variável corresponde a 497 dias. Portanto, se um equipamento passar mais que 497 dias sem ser desligado ou reiniciado, esta variável também será zerada. É interessante saber há quanto tempo um dispositivo está operacional. Muitas vezes descobrimos falhas em *software* ou *hardware* de equipamentos ao perceber que ele está reiniciando em curtos espaços de tempo.

10.4.3 Usando ping e traceroute

Apresentamos nesta seção algumas ferramentas que podem ser utilizadas para a obtenção do estado operacional de um equipamento.

A ferramenta mais usada para verificar o estado operacional de equipamento é o `ping`. A partir de uma estação qualquer, direcione `ping` para o equipamento cujo estado operacional você deseja obter:

```
maria@pc10:~$ ping 192.168.1.1
```

Se o dispositivo não responder ao `ping` pode-se concluir inicialmente que ele não está em operação no momento. Mas não se deve descartar a possibilidade de congestionamento de enlaces no caminho até o dispositivo, equipamentos sobrecarregados ou enlaces com problema.

Uma outra ferramenta que também pode ser utilizada para recuperar o estado operacional de um equipamento é o `traceroute`. Em máquinas com sistema operacional Windows esta ferramenta se chama `tracert`. Direcione `traceroute` ao equipamento cujo estado operacional você pretende obter:

```
maria@pc10:~$ traceroute -n 192.168.1.1

C:\WINNT> tracert –d 192.168.1.1
```

Os parâmetros `-n` e `-d` passados ao `traceroute` e `tracert` respectivamente indicam que a ferramenta não deve tentar mapear endereços para nomes de máquinas. Assim, o resultado do comando será mais rapidamente apresentado e não ficará dependente do sistema de resolução de nomes.

10.5 Obtendo estado operacional de interfaces

Neste procedimento descreveremos como recuperar o estado operacional de interfaces de rede.

10.5.1 Descrição e Dicas

O estado não operacional de uma interface pode indicar, dentre outras situações, que:

- a interface está administrativamente desativada;
- em geral, o estado administrativo de uma interface é comparado com seu estado operacional. Quando o estado administrativo (ver procedimento apresentado na Seção 10.13) não é igual ao estado operacional, algum problema pode estar ocorrendo;
- o equipamento ligado à interface está desligado ou com defeito;
- a interface está com defeito;
- tipicamente, duas falhas podem levar uma interface a ficar defeituosa: falhas no sistema de alimentação de energia elétrica e defeitos de *hardware*.

10.5.2 Usando uma estação de gerência SNMP

Nesta seção descreveremos que variável SNMP indica o estado operacional de interfaces. Além disso, dicas de configuração de notificações e alarmes para o estado operacional de interfaces serão dadas.

A variável **ifOperStatus** do grupo Interfaces da MIB-s [RFC2233] indica o estado operacional de uma interface. Esta variável pode assumir os seguintes valores:

- up(1) → indica que a interface está operacional, pronta para receber e transmitir quadros;
- down(2) → interface não operacional;
- testing(3) → interface está em modo teste;
- unknown(4) → por alguma razão a interface está em um estado indeterminado;

- dormant(5) → a interface não está em condições de transmitir quadros (não está no estado "up"). A interface está num estado "pendente", esperando a ocorrência de algum evento externo;
- notPresent(6) → algum componente da interface (em geral de *hardware*) está faltando. Este estado é um refinamento do estado "down";
- lowerLayerDown(7) → interfaces de camadas inferiores não estão operacionais, causando o estado não operacional da interface. É também um refinamento do estado "down";

No grupo Interfaces original da MIB-2 apenas os estados up(1), down(2) e testing(3) existiam. Se o estado administrativo de uma interface é up(1) (ver procedimento apresentado na Seção 10.5) e o estado operacional não é up(1), é provável que alguma condição de falha exista na rede.

Configure o agente SNMP dos equipamentos mais importantes da rede para gerar notificações (*traps*) para a estação de gerência quando o estado operacional das interfaces críticas mudar para "down" ou deixar de ser "down". O objeto ifLinkUpDownTrapEnable (grupo Interfaces da MIB-2 [RFC2233]) das interfaces críticas deve ser configurado com o valor "enabled(1)".

Uma outra forma de ser avisado quando o estado operacional de uma interface mudar é configurar alarmes e eventos em uma sonda RMON. Na Tabela 10-6 são apresentados alguns dados do alarme a ser configurado na sonda RMON:

O estado "up" desejado é representado na MIB pelo valor inteiro 1. O limiar crescente 2 é alcançado quando o estado da interface for outro diferente do desejado. Quando a interface voltar a funcionar o valor de ifOperStatus vai voltar a ser 1. O alarme deve gerar uma notificação (*trap*) para a estação de gerência quando os limiares crescente e decrescente forem atingidos.

Variável a ser monitorada:	ifOperStatus
Tipo:	absoluteValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	2
Limiar decrescente:	2

Tabela 10-6: Dados para configuração de alarme para mudança de estado operacional de uma interface.

10.5.3 Usando uma interface de linha de comando

Nesta seção apresentaremos comandos que podem ser executados em comutadores ou roteadores Cisco para a obtenção do estado operacional de interfaces. Se você possui equipamentos produzidos por outros fabricantes procure os comandos correspondentes aos apresentados nesta seção nos manuais do seu equipamento.

Na maioria dos roteadores Cisco, execute o seguinte comando:

```
show interfaces [tipo da interface] [número da interface]
```

A primeira linha da resposta a este comando informa o estado da interface. Veja um exemplo:

```
roteador# show interfaces FastEthernet 1/1/0
FastEthernet0 is down, line protocol is down
(…)
```

Esta linha indica que a interface Fast Ethernet 1/1/0 não está operacional. Se a interface estivesse administrativamente desabilitada, a primeira linha seria:

```
FastEthernet1/1/0 is administratively down, line protocol is down
```

Em comutadores Cisco execute o comando a seguir:

```
show port status [módulo[/porta]]
```

Este comando informa o estado das portas de um comutador. Veja um exemplo de sua execução:

```
Console> show port status

Port  Name               Status     Vlan      Duplex Speed  Type
----- ------------------ ---------- ---------- ------ ------ ------------
 1/1                     connected  2          half   100    100BaseTX
 1/2                     faulty                half   100    100BaseTX
 1/3                     inactive   4          half   100    100BaseTX
 1/4                     disabled              half   100    100BaseTX
```

O resultado do comando `show port status` indica que a porta 1/1 está operacional e que ela está conectada a um dispositivo também operacional; a porta 1/2 está defeituosa; a porta 1/3 está inativa porque pertence a uma VLAN inexistente e a porta 1/4 está administrativamente desabilitada.

10.5.4 Usando outras ferramentas de gerência

Em máquinas Unix-*like* você pode usar o comando `ifconfig` para verificar o estado de interfaces. Veja um exemplo do resultado do comando `ifconfig` abaixo:

```
root@servidor# ifconfig –a eth0
eth0 Link encap:Ethernet  HWaddr 00:60:94:63:6E:3A
     inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:658685 errors:0 dropped:0 overruns:0 frame:3
     TX packets:555222 errors:0 dropped:0 overruns:19 carrier:1
     collisions:44644 txqueuelen:100
     Interrupt:5
```

Analisando o resultado do comando `ifconfig`, concluímos que a interface eth0 está administrativamente ativa ("UP"), aceita endereços de difusão e *multicast* ("BROADCAST" e "MULTICAST") e que está operacional e não apresenta problemas ("**RUNNING**"). Portanto, o resultado de `ifconfig` para uma interface administrativamente ativa e em funcionamento deve sempre apresentar as palavras "UP" e "RUNNING". O `ifconfig` não informa quando o equipamento ligado à interface está desligado ou com defeito. Mesmo que não seja possível a comunicação com o equipamento remoto, o `ifconfig` informará que a interface está "up" e "running".

O `ifconfig` pode apresentar resultados muito diferentes do apresentado acima, que indicam outros erros. Por exemplo, que a interface não pôde ser encontrada ou que não é possível a comunicação com o dispositivo.

10.6 Obtendo utilização de CPU

Neste procedimento apresentaremos como obter a utilização média de CPU em roteadores, comutadores e hospedeiros.

10.6.1 Descrição e dicas

Este índice desempenho, geralmente calculado na forma de uma porcentagem, informa quanta capacidade de CPU um equipamento está utilizando. Uma utilização alta de CPU, em geral, é um indicativo de problema.

Monitorar utilização de CPU em roteadores é muito importante. Nestes equipamentos, utilizações de CPU elevadas podem comprometer tarefas críticas, como atualização dinâmica de rotas e processamento de pacotes.

Já os comutadores não utilizam a CPU para realizar a comutação de quadros [PERF&FAULT-CISCO], mas algumas outras atividades – por exemplo, o processamento das BPDUs para o cálculo da árvore de cobertura – são comprometidas devido a altas taxas de utilização de CPU.

É indispensável também monitorar a taxa de utilização de CPU em servidores. Quando a utilização de CPU nestas máquinas está elevada os clientes perceberão um mau desempenho das aplicações. Muitas vezes a equipe de gerência de aplicações ou até os usuários podem culpar a rede pelo mau desempenho das aplicações. Na realidade, muitos recursos além da rede podem estar causando a lentidão. Dentre eles encontram-se CPU, memória e disco.

Muitos são os fatores que podem aumentar a taxa de utilização de CPU em um servidor. Ele pode estar sendo alvo de ataque DoS, outra aplicação que não deveria estar sendo executada está tomando muito tempo de processador, ou ainda pode ser um indício de que o serviço está sendo muito requisitado e já é necessário alguma solução para o problema de saturação de capacidade de CPU.

O ideal é que você monitore as taxas de utilização de CPU dos equipamentos mais importantes da rede e estabeleça o seu próprio limiar. Uma utilização média de 75% de CPU é um sinal de advertência para que você fique atento e

já comece a analisar o porquê desta taxa. **90% de utilização média de CPU é alarmante.** Alguns equipamentos conseguem trabalhar com altas taxas de utilização de CPU sem degradar o seu desempenho, outros não.

É mais interessante calcular a utilização de CPU para intervalos de tempo maiores. Por exemplo, uma utilização de CPU média de 80% no último minuto não significa na realidade um sinal de advertência. Por coincidência podemos ter calculado a utilização de CPU em um momento em que a máquina estava realmente sobrecarregada. No entanto, se a utilização média de CPU mantém-se em 80% durante algumas dezenas de minutos, preocupe-se! Em resumo, se raramente a utilização é alta – esporadicamente calcula-se 90% de utilização de CPU – não há problema. Mas se a utilização de CPU alta se prolonga por dezenas de minutos, uma investigação deve ser realizada.

10.6.2 Usando uma estação de gerência SNMP

Nesta seção apresentamos variáveis SNMP que oferecem informações sobre a utilização de CPU de equipamentos.

Não existe uma MIB padrão – como a MIB-2, por exemplo – que informe a taxa de utilização de CPU de equipamentos de interconexão de redes. Em roteadores Cisco com versão de IOS inferior a 12.0(3)T, alguns objetos da MIB OLD-CISCO-SYSTEM [OLD-CISCO-SYSTEM-MIB] podem ser utilizados para a obtenção da taxa de utilização de CPU. Em roteadores com IOS mais recente, objetos da MIB CISCO-PROCESS [CISCO-PROCESS-MIB] podem ser utilizados. A MIB antiga considerava apenas um processador por equipamento. A nova MIB traz uma tabela com informações sobre todos os processadores. A semântica dos objetos não muda de uma MIB para outra. O que muda é o nome dos objetos e o tipo, pois em uma delas – na MIB mais recente – os objetos são colunares, isto é, fazem parte de uma tabela. Cada linha da tabela traz estatísticas de uso de um processador. A Tabela 10-7 descreve os objetos que lhe informam sobre utilização de CPU. Mais informações sobre obtenção de utilização de CPU em equipamentos Cisco usando SNMP são encontradas em [CPU-UTILIZATION-HOWTO].

OLD-CISCO-SYSTEM	CISCO-PROCESS	
busyPer	cpmCPUTotal5sec	A taxa de utilização média da CPU nos últimos 5 segundos.
avgBusy1	cpmCPUTotal1min	A taxa de utilização média da CPU no último minuto.
avgBusy5	cpmCPUTotal5min	A taxa de utilização média da CPU nos últimos 5 minutos.

Tabela 10-7: objetos que informam a utilização de CPU em roteadores Cisco.

Todos estes objetos já lhe dão o percentual de utilização dos processadores. Portanto, nenhum cálculo adicional precisa ser realizado. A variável que oferece a utilização média nos últimos 5 minutos deve ser usado para avaliação da utilização de CPU em equipamentos ao longo do dia. Caso você suspeite de que

em um determinado momento um equipamento está com utilização de CPU muito alta, podendo ser a causa de lentidão na rede, a utilização média de CPU em intervalos menores pode ajudar.

Se você possui roteadores de outro fabricante, busque informações sobre as MIBs suportadas na documentação do seu equipamento.

É importante que agentes SNMP estejam ativos em todos os servidores. Assim, podemos obter informações importantes de gerência via SNMP. Em servidores com agente SNMP instalado a MIB Host Resources [RFC1514] pode ser utilizada. O objeto `hrProcessorLoad` informa a taxa de utilização de CPU no último minuto.

10.6.3 Usando uma interface de linha de comando

Nesta seção mostramos alguns comandos que retornam a utilização de CPU em comutadores e roteadores Cisco.

Em comutadores Cisco mais novos você pode obter a taxa de utilização de CPU com o seguinte comando:

```
Console> (enable) show proc cpu
(W)CPU utilization for five seconds: 1.0%; one minute: 1. 0%; five
minutes: 1. %

PID  Runtime(ms)  Invoked  uSecs  5Sec   1Min   5min   TTY  Process
0    0            0        0      99.1%  99.0%  99.0%  0    idle
1    1            36       1000   0.0 %  0.0 %  0.0 %  0    Flash MIB Updat
2    1342         2846     46000  0.0 %  0.0 %  0.0 %  0    SynDiags
3    730172       4440594  40000  0.0 %  0.0 %  0.0 %  0    SynConfig
4    33752        424120   1000   0.0 %  0.0 %  0.0 %  0    Statuspoll
5    7413         44916    1000   0.0 %  0.0 %  0.0 %  0    SWPoll64bCnt
6    9568         1588983  1000   0.0 %  0.0 %  0.0 %  0    SL_TASK
7    746          636118   10500  0.0 %  0.0 %  0.0 %  0    RedundantTask
```

Em roteadores Cisco use o comando `show processes cpu` como exemplificado a seguir:

```
roteador1# show processes cpu

CPU utilization for five seconds: 3%/3%; one minute: 3%; five minutes: 2%

PID  Runtime(ms)  Invoked  USecs  5Sec   1Min   5Min   TTY  Process

1    6040         1602152  3      1.30%  1.20%  0.95%  0    Load Meter

2    63184        2449411  25     0.95%  1.05%  0.85%  0    Load Meter

3    4840624      813473   5950   0.65%  0.60%  0.15%  0    Check heaps

4    0            1        0      0.10%  0.15%  0.05%  0    Chunk Manager

(…)
```

Se no seu roteador for verificada uma taxa elevada de CPU, descubra que processo está consumindo mais CPU.

Se o seu roteador/comutador não for fabricado pela Cisco, procure o comando que dá informações sobre os processadores na documentação do seu equipamento.

10.6.4 Usando top e vmstat

Em máquinas Linux vários comandos informam a utilização de CPU. A seguir serão apresentados dois comandos bastante utilizados para a análise da utilização de CPU: o `top` e o `vmstat`.

EM AMBIENTE LINUX

O comando `top` oferece informações diversas sobre o sistema. Além de informar a média de utilização de CPU, o comando também informa quanta CPU cada processo em execução está consumindo. Um exemplo da saída do comando `top` segue:

```
maria@server:~$ top –d 300
8:42pm  up 140 days,  4:35,  2 users,  load average: 3.31, 3.45, 3.66
68 processes: 59 sleeping, 9 running, 0 zombie, 0 stopped
CPU states: 97.7% user,  2.2% system,  0.0% nice,  0.0% idle
Mem:  255772K av,  249484K used,  6288K free,  0K shrd,  2360K buff
Swap:  530136K av,  3828K used,  526308K free  36616K cached

PID    USER  PRI  NI   SIZE  RSS  SHARE STAT  LIB  %CPU  %MEM  TIME   COMMAND
24462  ftp   16   0    260   16   4     R     0    38.2  00.0  8934m  in.ftpd
20259  root  10   0    19044 18M  1160  S     0    34.4  7.4   2:33   netmngr
22234  root  20   0    10916 10M  1156  R     0    13.5  4.2   0:40   netmngr
12200  root  9    0    22464 20M  780   R     0    0.2   8.2   46:58  named
1      root  8    0    72    64   44    S     0    0.0   0.0   0:04   init
(…)
```

No exemplo acima percebe-se que a CPU está com mais de 85% de utilização média nos últimos 300 segundos. As aplicações `in.ftpd` e `netmngr`, juntas, consumiram mais 85% da capacidade de CPU durante este intervalo de tempo. Cabe a você e à sua equipe decidir se há ou não um problema e, se houver, como corrigi-lo. Não é bom ter um servidor com 100% de utilização sempre. Mas se esta utilização alta é esporádica a alta taxa de utilização não é tão alarmante. Por *default*, de 5 em 5 segundos as estatísticas oferecidas pelo comando `top` são atualizadas[60]. Para uma avaliação diária, como já comentamos anteriormente, é mais interessante obter a utilização média de CPU para um intervalo maior. Por isso, no exemplo dado, passamos o parâmetro 300 para o comando `top`. Ele indica que as atualizações só serão feitas a cada 5 minutos e portanto refletirão a utilização média de CPU neste intervalo de tempo. Se você preferir pode aumentar este intervalo para algumas dezenas de minutos.

Um outro comando que pode ser utilizado é o `vmstat`:

```
maria@server:~$ vmstat 300
procs     memory                  swap      io        system     cpu
r  b  w   swpd  free   buff  cache si   so  bi   bo   in   cs    us  sy  id
0  0  0   3008  21856  1828  33508 0    0   1    4    2    1     20  3   77
1  0  0   3008  21860  1828  33508 0    0   1    26   145  111   19  2   78
```

[60] Use o comando interativo `q` para sair das estatísticas `top`.

```
0  0  0  3008 21352 1828 33512 0   0   0    0    145  128  28 3  69
0  0  0  3008 22348 1828 33516 0   0   0    0    141  113  26 4  70
0  0  0  3008 22348 1828 33516 0   0   0    0    124  77   11 3  86
2  0  0  3008 11188 1840 35456 0   0   389  26   156  41   68 1  31
```

Como o parâmetro 300 é passado para o comando `vmstat`, uma linha com as estatísticas atualizadas é adicionada a cada cinco minutos (300 segundos).

A primeira linha apresenta estatísticas médias desde a última reinicialização da máquina. As demais linhas são adicionadas uma a uma, a cada 5 segundos. Este intervalo de tempo foi passado como parâmetro para o comando `vmstat`. Se nenhum parâmetro tivesse sido passado apenas a primeira linha seria apresentada. A partir da segunda linha as estatísticas apresentadas correspondem ao intervalo de tempo passado como parâmetro. Observe as 3 últimas colunas. Elas oferecem informações sobre a utilização da CPU. Durante o intervalo de tempo que se passou, qual a porcentagem de utilização de CPU consumida por processos de usuários e por processos do sistema operacional. A última coluna informa a porcentagem de tempo durante o qual a CPU ficou inativa.

EM AMBIENTE WINDOWS

Em máquinas Windows 2000 podemos gerar um gráfico que apresente a utilização de CPU ao longo do dia. No menu Iniciar escolha Programas > Ferramentas Administrativas > Desempenho. Na tabela de contadores (painel inferior direito) clique com o botão direito do mouse e escolha o item Adicionar Contadores. Em seguida escolha o contador Processor Time relacionado ao processador: Veja na Figura 10-1 um gráfico de utilização de CPU gerado desta forma.

10.7 Obtendo utilização de memória em roteadores e comutadores

Neste procedimento informaremos como podemos obter a utilização de memória em roteadores e comutadores.

10.7.1 Descrição e dicas

A utilização de memória, geralmente expressa como um percentual, informa quanta memória um equipamento está utilizando em comparação com a utilização máxima de memória do equipamento, que teoricamente é, 100%.

Roteadores e comutadores armazenam em memória principal os processos em execução. Mas, ao contrário de hospedeiros, em roteadores e comutadores não existem técnicas que possam "expandir" a memória principal.

Quando um roteador não possui recursos suficientes para processar um datagrama – não há *buffers* livres, por exemplo – o datagrama é descartado, mesmo que não apresente erros. Portanto, é comum que encontremos limitações de memória em um roteador ao descobrir um número elevado de descartes.

Em roteadores e comutadores a dica é a seguinte:

- a partir de 75% de utilização de memória (em longo prazo) fique atento. Este é um sinal de advertência;
- o limiar de alarme fica em torno de 90%-95% de utilização de memória em longo prazo.

Uma outra regra geral é: observe a utilização de memória de seus roteadores e comutadores e estabeleça seu próprio limiar. Se um roteador apresenta constantemente utilização de 1% de memória e de repente começa a apresentar utilização de 20%, investigue. Apesar deste número não ser elevado e não ser um limiar geral, é um número muito maior que o constantemente obtido e é, muito provavelmente, um indicativo de problema.

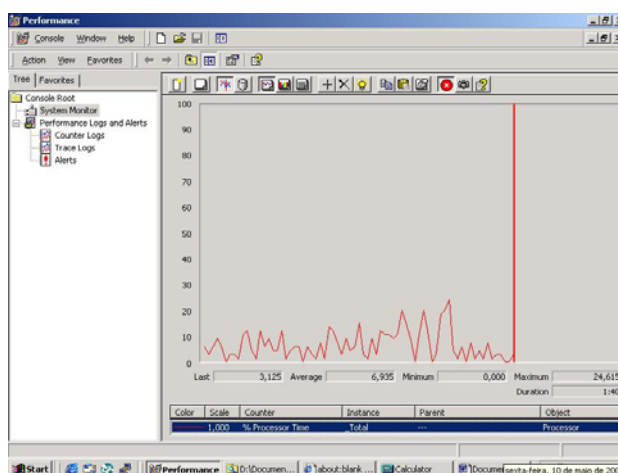



Figura 10-1: Estatísticas de uso de CPU no Windows.

10.7.2 Usando uma estação de gerência SNMP

Nesta seção apresentamos algumas variáveis SNMP que trazem informações sobre o uso de memória em roteadores e comutadores. Mostraremos também variáveis que informam a quantidade de quadros descartados por um equipamento de interconexão devido à limitação de recursos.

A MIB CISCO-MEMORY-POOL, proprietária da Cisco, oferece uma tabela, chamada ciscoMemoryPoolUtilizationTable, que indica a utilização média de memória em um roteador em períodos de tempo de 1, 5 e 10 minutos. Esta tabela é um incremento da tabela ciscoMemoryPoolTable da qual falaremos mais adiante. Nestas tabelas existe uma linha com estatísticas de alocação de memória para cada tipo de memória existente no roteador. A Cisco definiu 5 tipos de memória. Dentre elas estão a memória de processador, que deve existir em todos os dispositivos, e a memória de entrada e saída. As variáveis ciscoMemoryPoolUtilization1Min, ciscoMemoryPoolUtilization5Min e ciscoMemoryPoolUtilization10Min indicam a utilização de cada tipo de memória nos últimos 1, 5 e 10 minutos respectivamente. Informações mais detalhadas podem ser encontradas em [CISCO-MEMORY-POOL-MIB].

Outras variáveis SNMP importantes para a monitoração de utilização de memória em roteadores Cisco [CISCO-MEMORY-POOL-MIB, OLD-CISCO-MEMORY-MIB] são:

- ciscoMemoryPoolFree, objeto colunar da tabela ciscoMemoryPoolTable da MIB CISCO-MEMORY-POOL ou freeMem variável da OLD-CISCO-MEMORY. Estas variáveis indicam o número de bytes livres na memória do equipamento. O objeto freeMem é obsoleto, mas ainda precisa ser usado para a recuperação da quantidade de memória livre em roteadores Cisco com IOS inferior à versão 11.1;

- ciscoMemoryPoolUsed, objeto colunar da tabela ciscoMemoryPoolTable da MIB CISCO-MEMORY-POOL. Esta variável indica o número de bytes em uso da memória do equipamento;

- ciscoMemoryPoolLargestFree, objeto colunar da tabela ciscoMemoryPoolTable da MIB CISCO-MEMORY-POOL. Indica a quantidade máxima de bytes contíguos livres na memória. Este valor é sempre menor ou igual ao valor indicado pela variável ciscoMemoryPoolFree. O limiar mínimo recomendado para esta variável é 500KB [PERF&FAULT-CISCO];

- bufferNoMem da MIB OLD-CISCO-MEMORY. Esta variável conta o número vezes que a tentativa de criação de um *buffer* falhou devido à falta de memória. Quando este contador aumenta um datagrama é provavelmente descartado.

Para obter a utilização de memória com base nestas variáveis precisamos comparar a quantidade de memória em uso com a quantidade total de memória no sistema. Isto pode ser feito segunda a Equação 10.7-1 ou a Equação 10.7-2:

$$\text{Utilização de memória (\%)} = \frac{\text{Qtde. total de memória} - \text{Qtde. de memória livre}}{\text{Qtde. total de memória}} \times 100$$

Equação 10.7-1

$$\text{Utilização de memória (\%)} = \frac{\text{Qtde. de memória em uso}}{\text{Qtde. total de memória}} \times 100$$

Equação 10.7-2

Como mencionado na Seção **DESCRIÇÃO E DICAS**, datagramas são descartados devido a falta de recursos para processá-los, incluindo falta de memória. É importante, portanto, que monitoremos a quantidade de descartes devido a falta de recursos em um equipamento. Para tal, variáveis do grupo Interfaces da MIB-2 podem ser utilizadas [RFC2233]:

- ifInDiscards é um contador incrementado cada vez que um quadro que chega em uma interface, ainda que correto, tem que ser descartado devido à falta de recursos, como por exemplo, não há memória disponível;

- ifOutDiscards é um contador incrementado cada vez que um quadro, ainda que correto, não pode ser transmitido por uma interface devido a falta de recursos, como, por exemplo, falta de memória.

Estes contadores não devem ser incrementados com freqüência, e sua taxa de crescimento deve ser bem menor que a taxa de crescimento de entrada e saída de quadros da interface.

10.7.3 Usando uma interface de linha de comando

Nesta seção mostraremos comandos que podem ser executados na interface de linha de comando de comutadores e roteadores Cisco para a obtenção de informações relacionadas à utilização de memória no equipamento. Em equipamentos de outros fabricantes devem existir comandos correspondentes. Busque informações no manual do seu equipamento.

Em roteadores Cisco com versão de IOS superior a 10.0 os seguintes comandos podem ser executados:

```
show memory [memory-type] [free] [summary]
show processes memory
```

Vejamos primeiro um exemplo da execução do comando `show memory`:

```
roteador> show memory
               Head    Total(b)    Used(b)    Free(b)   Lowest(b)  Largest(b)
Processor  61345760   248228000   16818760  231409240   231201272   230393684
   Fast    61325760      131080      24664     106416      106416      106364
(…)
```

A primeira seção do resultado do comando `show memory` é uma tabela (que pode ser vista no exemplo de execução apresentado) bastante interessante. Ela oferece estatísticas gerais de uso de cada um dos tipos de memória suportados pelo roteador (neste caso Procecssor e Fast). A Tabela 10-8 explica algumas das colunas desta tabela.

Campo	Descrição
Total(b)	Quantidade total de bytes na memória (soma de bytes disponíveis e em uso da memória).
Used(b)	Quantidade de bytes da memória em uso.
Free(b)	Quantidade de bytes livres da memória.
Lowest(b)	Quantidade de memória livre (em bytes) no momento de maior utilização de memória desde a inicialização do equipamento.
Largest(b)	Tamanho em bytes do maior bloco livre da memória.

Tabela 10-8 Descrição de alguns campos do resultado do comando show memory.

Veja a seguir o resultado do comando `show processes memory`:

```
roteador>show proc mem
Total: 248228000, Used: 16820540, Free: 231407460
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
```

```
   0   0     446636      65836   13942472          0          0 *Init*
   0   0        912     686860        912          0          0 *Sched*
   0   0   19590060    5218804      40688    5445248          0 *Dead*
   1   0        268        268       3796          0          0 Load Meter
   2   0       6476   63247816       7296          0          0 OSPF Hello
   3   0          0          0       6796          0          0 Check heaps
   4   0      21972          0      28768          0          0 Chunk Manager
   5   0         96          0       6892          0          0 Pool Manager
   6   0        268        268       6796          0          0 Timers
(…)
                                 16815220 Total
```

Inicialmente, este comando informa a quantidade total de memória no sistema e as quantidades de memória livre e em utilização no momento de sua execução. Em seguida uma tabela com os processos que estão carregados na memória é apresentada. Os campos Allocated, Freed e Holding são explicados na Tabela 10-9.

Campo	Descrição
Allocated	Quantidade de bytes da memória alocados para o processo.
Freed	Quantidade de bytes da memória liberados pelo processo, independente de os tenha alocado.
holding	Quantidade de memória correntemente em uso pelo processo.

Tabela 10-9: Descrição de alguns campos da tabela apresentada pelo comando show processes memory.

Na maioria dos comutadores Cisco o comando a seguir pode ser executado:

```
show proc [cpu | mem]
```

O procedimento apresentado na Seção 10.6 mostra o resultado deste comando com o parâmetro `cpu`. A seguir, veja o resultado deste comando com o parâmetro `mem`:

```
Console> (enable) show proc mem

Total: 10945712, Used: 1438992, Free: 9506720
PID TTY Allocated Freed  Holding Process
0   0   706240    2832   703408  idle
1   0   240       0      240     Flash MIB Updat
2   0   164944    164144 800     SynDiags
3   0   208224    2992   205232  SynConfig
4   0   96        0      96      Statuspoll
5   0   2592      2560   32      SWPoll64bCnt
6   0   80        0      80      SL_TASK
7   0  2272      1952   320     RedundantTask
```

O resultado deste comando oferece estatísticas gerais de uso da memória e estatísticas de alocação da memória por processo. Os campos desta tabela podem ser interpretados como mostrado na Tabela 10-9.

10.8 Obtendo utilização de memória em hospedeiros

Neste procedimento informaremos como podemos obter a utilização de memória em hospedeiros.

10.8.1 Descrição e dicas

A utilização de memória, geralmente expressa como um percentual, informa quanta memória um equipamento está utilizando em comparação com a utilização máxima de memória do equipamento, que teoricamente é, 100%.

Os sistemas operacionais atuais estendem a memória principal através de paginação e do conceito de memória virtual. Com o uso destes métodos é possível que o tamanho dos processos em execução em um determinado momento seja maior que o tamanho da memória principal, e ainda que o tamanho de um único processo seja maior que o tamanho da memória principal.

Para estender a memória principal, o sistema operacional faz uso de uma área do disco rígido para armazenar temporariamente páginas (pedaços de processos em execução), geralmente chamada área de *swap*. Ao transporte de uma página que estava no disco rígido para a memória principal chamamos *page in*. O transporte inverso chama-se *page out*. Para que um processo seja executado não é necessário que ele, seus dados e sua pilha estejam na memória por completo. Basta que esteja em memória principal apenas as partes que estão realmente em uso no momento. O restante dele fica na área de *swap* e é trazido para a memória principal quando necessário.

O transporte de páginas da memória para o disco de um processo que ainda está em execução apenas para liberar espaço em memória para novas páginas deste ou de outro processo (*page out*) só é necessária quando a soma dos tamanhos dos processos em execução ultrapassa a capacidade de armazenamento da memória principal. A realização constante de *page in* e *page out* pode comprometer o desempenho do sistema. Assim, o limiar de utilização de memória em um hospedeiro não é medido pela utilização da memória em si, mas pela freqüência de paginação. Se você perceber que o sistema operacional está fazendo paginação sempre, uma investigação mais detalhada deve ser realizada. Caso o paginação só ocorra esporadicamente, você não tem problemas de memória.

10.8.2 Usando uma estação de gerência SNMP

Nesta seção apresentamos algumas variáveis SNMP que trazem informações sobre o uso de memória em hospedeiros.

Em hospedeiros com agentes SNMP instalados, podemos obter informações sobre a utilização de memória através de objetos da MIB de Recursos do Hospedeiro (*Host Resources MIB*) [RFC1514]. Cada linha da tabela hrStorageTable traz informações de uso de um determinado tipo de dispositivo de armazenamento. Através de objetos colunares desta tabela podemos obter informações de uso da memória principal e da memória virtual de um hospedeiro. A seguir mostramos alguns objetos colunares desta tabela:

- **hrStorageType** indica o tipo de memória cuja utilização está sendo reportada. Neste procedimento estamos interessados em memórias do tipo **hrStorageRam** e **hrStorageVirtualMemory**;

- **hrStorageAllocationUnits** informa a quantidade de bytes contidos em cada unidade de alocação da memória;

- **hrStorageSize** indica a quantidade total de unidade de alocação contidas na memória;

- **hrStorageUsed** informa a quantidade corrente de unidades de alocação da memória em uso;

- **hrStorageAllocationFailures** conta quantas vezes um pedido de alocação de memória não foi atendido devido a falta de recursos.

Com estas informações podemos obter a utilização de memória de um hospedeiro, como mostrado na Equação 10.7-2. Muitas informações sobre utilização de memória estão disponíveis na MIB Host Resources, mas infelizmente, a informação que mais nos interessa – que é a taxa de *page out* - não está lá.

10.8.3 Usando top

Neste procedimento mostraremos como obter a utilização de memória em hospedeiros com sistema operacional Linux ou Windows NT/2000.

EM AMBIENTE LINUX

O comando `top` oferece informações diversas sobre o sistema. Além de oferecer estatísticas sobre a utilização de memória total do sistema, este comando também informa quanta memória cada processo em execução está consumindo. Um exemplo da saída do comando `top` segue:

```
maria@server:~$ top
8:42pm  up 140 days,  4:35,  2 users,  load average: 3.31, 3.45, 3.66
68 processes: 59 sleeping, 9 running, 0 zombie, 0 stopped
CPU states: 97.7% user,  2.2% system,  0.0% nice,  0.0% idle
Mem:  255772K av,  249484K used,  6288K free,  0K shrd,  2360K buff
Swap:  530136K av,  3828K used,  526308K free  36616K cached
PID    USER  PRI  NI   SIZE   RSS  SHARE  STAT  LIB  %CPU  %MEM  TIME   COMMAND
24462  ftp   16   0    260    16   4      R     0    38.2  00.0  8934m  in.ftpd
20259  root  10   0    19044  18M  1160   S     0    34.4  7.4   2:33   netmngr
22234  root  20   0    10916  10M  1156   R     0    13.5  4.2   0:40   netmngr
12200  root  9    0    22464  20M  780    R     0    0.2   8.2   46:58  named
1      root  8    0    72     64   44     S     0    0.0   0.0   0:04   init
(…)
```

A primeira linha em destaque traz informações sobre a memória principal. Inclui quantidade de memória total, disponível, em uso, compartilhada e usada para *buffers*. Na segunda linha em destaque encontram-se estatísticas relacionadas à

área de *swap*, incluindo o tamanho total desta área, e quanto desta área está livre e em uso. Estas duas linhas são exatamente o resultado do comando `free`.

Com o comando `top` podemos estatísticas gerais de uso da memória e da área de *swap* e podemos descobrir que processos estão consumindo mais memória. Olhe como está a utilização da área de *swap*. Quando não passamos nenhum parâmetro para o comando `top`, a tela com estatísticas é atualizada a cada 5 segundos.

Um que traz informações mais precisas e interessantes sobre ocorrência de *swap* e utilização da memória é o `vmstat`. Veja uma saída típica deste comando:

```
maria@server:~$ vmstat 5
 procs          memory            swap      io      system       cpu
 r b w  swpd  free  buff cache  si  so   bi   bo   in   cs  us  sy  id
 1 2 0  2592  2164 75204 25404   0   2 1368   28  457  706  20  10  70
 0 0 0  2580  2144 75204 25124   2   0    7   10  121   42  23   1  77
 3 0 0  2580  1928 75204 24972   0   0    8   13  125   38  13   3  84
 2 0 0  2580  1120 75204 25300   0   0   91    3  156  107  48  33  19
 1 0 0  2604  1132 74460 26524   0   5 1198   16  148   56  48  45   6
 1 0 0  2604  1136 68336 33188   0   0  302 2542  177  132  11  40  49
 0 0 0  2604 19768 63284 20768   0   0   10    6  123   38  13  21  66
 0 0 0  2604 19680 63348 20788   0   0    0   16  123   29  12   1  87
 0 0 0  2604 19672 63348 20788   0   0    0    7  111   17  13   1  86
 0 0 0  2600 19704 63348 20760   1   0    0   29  115   23  10   1  89
 1 0 0  2596 19616 63412 20788   1   0    2    5  114   22  15   1  84
 0 1 0  2588 19584 63412 20808   2   0    1  890  142   79  27   2  72
```

A primeira linha apresenta estatísticas médias desde a última reinicialização da máquina. As demais linhas são adicionadas uma a uma, a cada 5 segundos. Este intervalo de tempo foi passado como parâmetro para o comando `vmstat`. Se nenhum parâmetro tivesse sido passado apenas a primeira linha seria apresentada. A partir da segunda linha as estatísticas apresentadas correspondem ao intervalo de tempo passado como parâmetro.

Observe especialmente as colunas `memory` e `swap`. Elas oferecem informações sobre a utilização da memória e sobre ocorrências de *swap*. Os sub-campos deste comando diretamente relacionados à utilização de memória são apresentados na Tabela 10-10.

Campo	Sub-campos	Descrição
Procs	w	Número de processos levados para a área de swap (em disco) mas que estão em execução.
Memory	swpd	Quantidade de memória virtual em uso (KB).
	free	Quantidade de memória livre (KB).

	buff	Quantidade de memória usada como buffers (KB).
Swap	si	Quantidade de memória transportada do disco para a memória (KB/s).
	so	Quantidade de memória transportada da memória para o disco (KB/s).

Tabela 10-10 Descrição de sub-campos do resultado do comando vmstat.

EM AMBIENTE WINDOWS

Em máquinas Windows 2000 podemos gerar gráficos que mostrem *page outs*/s ao longo do dia e memória disponível. No menu Iniciar escolha Programas > Ferramentas Administrativas > Desempenho. Na tabela de contadores (painel inferior direito) clique com o botão direito do mouse e escolha o item Adicionar Contadores. Em seguida escolha os seguintes contadores relacionados à memória: Available MBytes e Pages Output/sec. Veja um gráfico de page out/s e memória disponível gerado pelo Windows 2000 na Figura 10-2.

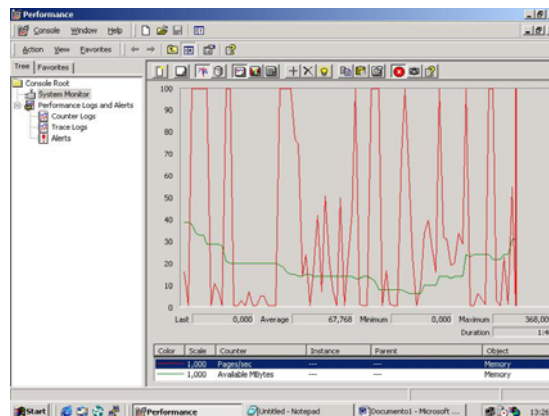



Figura 10-2: Gráfico de desempenho gerado pelo Windows com contadores de *page out*/s e memória disponível.

10.9 Analisando quantidade de tráfego de *broadcast* e *multicast*

Neste procedimento analisaremos a quantidade de tráfego de *difusão* e *multicast* em um domínio de difusão.

10.9.1 Descrição e dicas

Um quadro de *broadcast* (quadro de difusão) é um quadro endereçado a todas as estações que fazem parte do mesmo domínio de difusão do emitente do quadro. Muitos serviços de rede dependem de quadros de difusão para seu funcionamento. Dentre estes serviços encontram-se:

- ARP, para mapear endereços IP em endereços MAC;

- RARP, usado para mapear endereços MAC em endereços IP;
- RIP, divulga rotas através de quadros de difusão;
- DHCP (e BOOTP), para requisitar endereços IP e fornecer respostas;
- NETBIOS, para divulgar serviços, localizar serviços, implementar *logon* e implementar navegação em arquivos através da rede.

Alguns destes serviços (ARP, por exemplo) enviam quadros de difusão nível 2 – onde o endereço de difusão físico é usado – e outros enviam quadros de difusão nível 3 (DHCP, por exemplo) – onde o endereço de difusão lógico (255.255.255.255) é usado. Um quadro cujo endereço destino físico é o de difusão (FFFFFFFFFFFF) carrega um datagrama IP cujo endereço destino é de difusão lógico ou não carrega datagrama IP algum. No primeiro caso há difusão nível 3 e no seguindo nível 2.

Um quadro *multicast* é um quadro endereçado a um subconjunto de todas as máquinas da rede. Um datagrama IP com endereço destino *multicast* vai atravessar roteadores ao longo de seu caminho. É possível que um roteador intermediário precise copiar este datagrama e transmiti-lo para vários outros roteadores. Quando o datagrama *multicast* chega a um roteador que dá acesso a máquinas que desejam receber esse datagrama, o roteador encapsula o datagrama em um quadro com endereço físico destino *multicast* e o transmite. Esse quadro vai ser transmitido em um domínio de difusão e um comutador que o receber poderá transmiti-lo para várias de suas portas para que ele chegue em todos os seus destinos. Exemplos de serviços que usam *multicast* são: Cisco Discovery Protocol, OSPF, vídeo-conferência e outras aplicações multimídia.

Ao receber um quadro de *broadcast*, um comutador o encaminha para todas as máquinas que fazem parte da VLAN do emissor, atingindo assim todas as máquinas do domínio de difusão. Cada equipamento na rede deve receber e processar o quadro, mesmo que não tenha interesse no mesmo.

A existência de quadros de difusão e *multicast* na rede é absolutamente normal. Mas, quando a quantidade de quadros de *broadcast/multicast* em uma rede está muito alta dizemos que está ocorrendo uma tempestade de difusão. Em geral, queremos monitorar o tráfego de *broadcast* da rede porque um tráfego de difusão muito alto pode saturar os processadores dos equipamentos da rede. É isso mesmo: em geral, o efeito negativo de uma tempestade de difusão não é a saturação dos enlaces da rede, mas sim a saturação dos processadores dos equipamentos da rede.

Já vimos na literatura de gerência de redes que no backbone, em horários normais de tráfego, aceita-se que o tráfego de *broadcast/multicast* consuma até uns 20% da largura de banda dos enlaces. Não achamos esta forma de analisar o tráfego de broadcast e *multicast* na rede interessante. A quantidade de largura de banda consumida por tráfego de difusão depende de vários fatores, dentre eles: o tipo das aplicações sendo utilizadas na rede, o sistema operacional de rede, os protocolos utilizados e o horário em que o tráfego está sendo medido. À noite, por exemplo, quase todo o tráfego da rede será resumido a tráfego de *broadcast/multicast*. Por depender de tantos fatores intrínsecos de uma

determinada rede, não consideramos adequado se falar em percentual máximo aceitável de tráfego de *broadcast/multicast*. Determinar este percentual é uma tarefa complexa e envolve todos os fatores mencionados.

Achamos mais interessante estabelecer limiares para a quantidade de quadros de *broadcast/multicast* por segundo. Equipamentos de tecnologia mais recente podem processar algumas centenas de quadros *broadcast/multicast* por segundo sem afetar seu desempenho. No entanto, na prática, estabelecemos limiares menores, entre 100 e 200 quadros de difusão por segundo.

Para ter uma idéia do que ocorre com a utilização de CPU de um PC com processador Pentium de 120 MHz e placa de rede 3com Fast Etherlink quando o número de quadros de broadcast/multicast por segundo aumenta veja a Tabela 10-11 [DESIGNING-CISCO]:

Número de quadros *broadcast/multicast* recebidos por segundo	Consumo de CPU
100	2%
1300	9%
3000	25%

Tabela 10-11: Consumo de capacidade de CPU provocado pelo recebimento de quadros de difusão.

É possível identificar tempestades de difusão sem a utilização de quaisquer ferramentas de gerência. Observe os LEDs de dados das portas do comutador. Durante tempestades de difusão todos os LEDs de atividade nas portas piscam ao mesmo tempo muitas vezes em curtos espaços de tempo. Algumas vezes chegamos a ter a impressão de que os LEDs estão constantemente acesos durante algum tempo. Esta é uma forma *ad hoc* de identificar tempestades de difusão. Para certificar-se de que a tempestade está ocorrendo é necessário realizar alguns cálculos, que nos informe a quantidade média de quadros de difusão por segundo que trafega na rede.

A quantidade média de quadros *broadcast* e *multicast* por segundo em uma rede pode ser calculado segundo a Equação 10.9-1 e a Equação 10.9-2:

Equação 10.9-1

Equação 10.9-2

É possível ainda que as equações acima sejam unidas em uma única equação que ofereça a quantidade de quadros de *broadcast* e *multicast* que trafegam na rede por segundo. Veja a Equação 10.9-3:

$$\text{Multicasts/Broadcasts por segundo} = \frac{\text{Qtde. de quadros multicast e broadcast recebidos e transmitidos em } \Delta T}{\text{Qtde. de segundos em } \Delta T}$$

Equação 10.9-3

Na realidade, as informações sobre o tráfego de difusão são obtidas por interface. Desta forma, podemos separar o tráfego de difusão em tráfego de entrada e saída: quantidade de quadros de *broadcast* recebidos por segundo, quantidade de quadros de *broadcast* transmitidos por segundo e assim por diante. Esta separação é bastante interessante, porque durante uma tempestade de difusão podemos ter uma idéia de onde os quadros de difusão estão vindo. Veja as equações a seguir:

$$\text{Broadcasts por segundo}_{in} = \frac{\text{Qtde. de quadros broadcast recebidos em } \Delta T}{\text{Qtde. de segundos em } \Delta T}$$

Equação 10.9-4

$$\text{Broadcasts por segundo}_{out} = \frac{\text{Qtde. de quadros broadcast transmitidos em } \Delta T}{\text{Qtde. de segundos em } \Delta T}$$

Equação 10.9-5

$$\text{Multicasts por segundo}_{in} = \frac{\text{Qtde. de quadros multicast recebidos em } \Delta T}{\text{Qtde. de segundos em } \Delta T}$$

Equação 10.9-6

$$\text{Multicasts por segundo}_{out} = \frac{\text{Qtde. de quadros multicast transmitidos em } \Delta T}{\text{Qtde. de segundos em } \Delta T}$$

Equação 10.9-7

É interessante que uma estação de gerência apresente um gráfico do tráfego de quadros de *broadcast* e *multicast* por segundo pelo menos nos enlaces de *backbone*. Nas seções a seguir veremos como obter os termos das equações apresentadas nesta seção.

10.9.2 Usando uma estação de gerência SNMP

Nesta seção veremos como obter o tráfego de quadros de *broadcast*/*multicast* em uma rede com o auxílio de uma estação de gerência SNMP. Será também apresentado como configurar um alarme RMON que dispare quando a quantidade de quadros de difusão da rede for muito grande.

Alguns dos objetos que informam a quantidade de quadros de *broadcast*/*multicast* em uma rede já foram mencionados em procedimentos passados. Eles fazem parte do grupo Interfaces da MIB-2 [RFC2233]. São eles: **ifInBroadcastPkts**, **ifOutBroadcastPkts**, **ifInMulticastPkts** e **ifOutMulticastPkts**. No antigo grupo Interfaces da MIB-2 [RFC1213], apenas dois objetos são utilizados: **ifInNUcastPkts** e **ifOutNUcastPkts**. Todos estes objetos são do tipo contador. As variações destes contadores no tempo significam:

- **ΔifInBroadcastPkts** é a quantidade de quadros com endereços destino *broadcast* que chegaram na interface durante um certo intervalo de tempo e foram entregues a protocolos da camada superior;

- **ΔifInMulticastPkts** é a quantidade de quadros com endereços destino *multicast* que chegaram na interface durante um certo intervalo de tempo e foram entregues a protocolos da camada superior;

- **ΔifOutBroadcastPkts** é a quantidade total de quadros com endereços destino *broadcast* cuja transmissão foi solicitada por protocolos de nível superior em um determinado intervalo de tempo. São incluídos também os quadros com endereço destino *broadcast* descartados ou não enviados;

- **ΔifOutMulticastPkts** é a quantidade total de quadros com endereços destino *multicast* cuja transmissão foi solicitada por protocolos de nível superior em um determinado intervalo de tempo. São incluídos também os quadros com endereço destino *broadcast* descartados ou não enviados;

- ΔifInNUcastPkts é o número de quadros com endereço destino *broadcast* ou *multicast* entregues a camadas superiores em um determinado intervalo de tempo;

- **ΔifOutNUcastPkts** é a quantidade total de quadros com endereços destino *broadcast* ou *multicast* cuja transmissão foi solicitada por protocolos de nível superior em um determinado intervalo de tempo. São incluídos também os quadros com endereço destino *broadcast* ou *multicast* descartados ou não enviados.

O denominador das equações apresentadas na Seção **DESCRIÇÃO E DICAS** de deve ser o número de segundos contidos entre duas coletas de dados SNMP.

Vejamos um exemplo:

- suponha que sua estação de gerência está coletando dados SNMP a cada 5 minutos (300 segundos);

- em um certo momento T0 os seguintes valores foram obtidos:

    - $\text{ifInBroadcastPkts}_0 = 1200$
    - $\text{ifOutBroadcastPkts}_0 = 600$
    - $\text{ifInMulticastPkts}_0 = 4$
    - $\text{ifOutMulticastPkts}_0 = 4$

- 5 minutos depois, em T1, os seguintes valores foram obtidos:

    - $\text{ifInBroadcastPkts}_1 = 20200$
    - $\text{ifOutBroadcastPkts}_1 = 30800$

- ifInMulticastPkts$_1$ = 34
- ifOutMulticastPkts$_1$ = 34

Substituímos os valores encontrados na Equação 10.9-1 e Equação 10.9-2 e obtivemos o seguinte:

$$\text{Broadcasts por segundo} = \frac{(20200 - 1200) + (30800 - 600)}{300} = 164 \text{ broadcasts por segundo}$$

$$\text{Multicasts por segundo} = \frac{(34 - 4) + (34 - 4)}{300} = 0{,}2 \text{ multicasts por segundo}$$

Note que a quantidade média de quadros de *broadcasts* por segundo trafegando na rede está começando a ficar alta. É interessante criar alarmes RMON que gerem eventos de notificação para a estação de gerência quando o número de quadros de broadcast e *multicast* por segundo estiver alto. Veja na Tabela 10-12 e na Tabela 10-13 alguns dados dos alarmes a serem configurados na sonda RMON:

Variável a ser monitorada:	ifInBroadcastPkts
Tipo:	deltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	60000
Limiar decrescente:	60000

Tabela 10-12: Dados para configuração de alarme para tráfego de quadros de broadcast de entrada.

Variável a ser monitorada:	ifOutBroadcastPkts
Tipo:	deltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	60000
Limiar decrescente:	60000

Tabela 10-13: Dados para configuração de alarme para tráfego de quadros de broadcast de saída.

Os mesmos alarmes podem ser configurados para quadros *multicast*. Configure os alarmes para enviar notificações para a estação de gerência quando os limiares crescente e decrescente forem excedidos.

10.9.3 Usando uma interface de linha de comando

Nesta seção, mostraremos quais comandos em roteadores e comutadores Cisco oferecem contadores de quadros de *broadcast* e *multicast*. Se você possui equipamentos produzidos por outro fabricante, procure nos manuais de seus equipamentos os comandos correspondentes aos apresentados aqui.

Em roteadores Cisco com versão de IOS 10.0 ou superior execute o seguinte comando:

```
show ip traffic
```

Veja um exemplo da resposta deste comando:

```
roteador> show ip traffic
IP statistics:
  Rcvd:  2593286165 total, 10600762 local destination
         0 format errors, 0 checksum errors, 885818 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 32532 with options
  Opts:  72 end, 1 nop, 4 basic security, 0 loose source route
         0 timestamp, 0 extended security, 3 record route
         0 stream ID, 0 strict source route, 32459 alert, 0 cipso
         0 other
  Frags: 0 reassembled, 1 timeouts, 226 couldn't reassemble
         496166 fragmented, 0 couldn't fragment
  Bcast: 58033 received, 12 sent
  Mcast: 1893437 received, 3482544 sent
(…)
```

Este comando oferece estatísticas sobre o tráfego IP do roteador. Ele não separa o tráfego por interface. O comando a seguir também pode ser utilizado em roteadores Cisco com IOS versão 10.0 ou superior:

```
interfaces [tipo da interface] [número da interface]
```

Este comando separa o tráfego por interface, mas apresenta apenas a quantidade de quadros de *broadcast* e *multicast* recebidos pela interface.

Em comutadores Cisco execute o comando a seguir:

```
show mac [módulo[/porta]]
```

O comando abaixo também pode ser executado em comutadores cisco com versão de software superior a 6.1:

```
show port mac [módulo]/porta]]
```

Veja um exemplo da execução do comando `show port mac`:

```
Console> show port mac 1
Port     Rcv-Unicast           Rcv-Multicast        Rcv-Broadcast
```

```
-------- -------------------- -------------------- --------------------
 1/1                  121200                    0                 5210
 1/2                    5800                    1                 2340
 1/3                  198210                    6                72150
 1/4                    3450                   10                 1120

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                   15230                    0                 2140
 1/2                    3280                    1               125910
 1/3                  190210                    4                12580
 1/4                    2160                    5                46780
(…)
```

Substitua os valores obtidos através da interface de linha de comando nas equações apresentadas na Seção **DESCRIÇÃO E DICAS**.

10.9.4 Usando um analisador de protocolos

Nesta seção veremos como obter o tráfego de *broadcast/multicast* por segundo com o auxílio de um analisador de protocolos.

Conecte o analisador de protocolos no domínio de difusão que você deseja estudar. Se for conectar o analisador em um comutador certifique-se de que está conectando o analisador na VLAN correta.

No Sniffer, da Network Associates, use a função de amostragem histórica para gerar um gráfico que apresente a quantidade de *broadcasts*/s e *multicasts*/s no tempo. Na Figura 10-3 encontra-se um gráfico de broadcasts/s gerado pelo Sniffer. Se você observar Na Seção UTILIZANDO UM ANALISADOR DE PROTOCOLOS você encontrará dicas de como utilizar esta funcionalidade. Você também pode optar por apenas observar o contador de quadros *broadcast* e *multicast* no painel de detalhes do Sniffer.

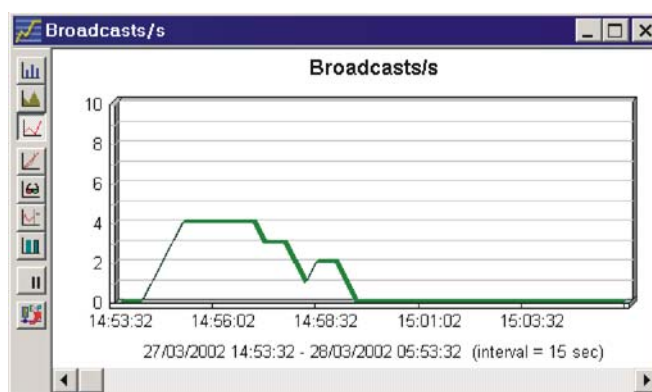



Figura 10-3: Gráfico de broadcasts/s gerado pelo Sniffer.

10.9.5 Usando outras ferramentas de gerência

Nesta seção veremos outras ferramentas que podem ser utilizadas em máquinas Windows para a obtenção do tráfego de *broadcast/multicast* na rede.

Use o comando `netstat` como exemplificado a seguir:

```
C:\WINNT>netstat -ne
Estatísticas de interface
                                   Recebido         Enviado
Bytes                                242119           30360
Pacotes unicast                         516             451
Pacotes não unicast                      24              32
Descartados                               1               1
Erros                                     2               0
Prot. Desconhecidos                      23
```

Com os dados obtidos você pode encontrar a média de quadros *broadcast/multicast* recebidos e transmitidos por segundo pela máquina em um determinado intervalo de tempo. Ver Equação 10.9-3.

10.10 Obtendo utilização de enlaces

Como calcular a utilização de enlaces? A partir de que valor consideramos a utilização de um enlace *half duplex* elevada? E de um enlace *full duplex*? Neste procedimento responderemos a todas estas questões.

10.10.1 Descrição e Dicas

Medir a utilização dos recursos da rede ajuda a descobrir quão congestionada ela está. Geralmente a utilização é calculada como uma percentagem, que é comparada à utilização máxima do recurso, que teoricamente é 100%. Neste procedimento você vai aprender como calcular a utilização de enlaces. Outros procedimentos indicam como calcular a utilização de CPU e de memória.

A utilização de enlaces é a medida mais utilizada para verificar a utilização de uma rede. Na prática, após uma certa taxa de utilização de enlace, o desempenho da rede fica comprometido. O gráfico apresentado na Figura 10-4 mostra uma curva típica do tempo de resposta em função da utilização do enlace.

Figura 10-4: gráfico tempo de resposta x utilização de enlaces.

Este gráfico apresenta um joelho. Com utilização menor que o joelho (uns 70% para segmentos com acesso ao meio não compartilhado), o desempenho médio e a variabilidade do tempo de resposta são bons. No entanto, com utilização maior que o joelho, a média e a variabilidade ficam bem piores. Veja o gráfico da Figura 10-5. Após uma certa taxa de utilização do enlace (o joelho do gráfico), ao aumentar um pouco a utilização o aumento do tempo de resposta correspondente é bastante grande.

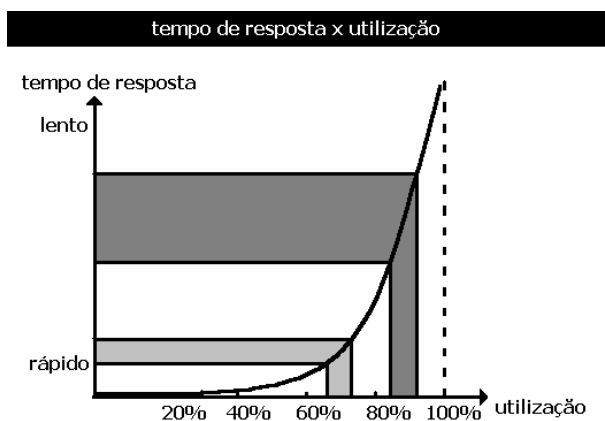



Figura 10-5: variabilidade do tempo de resposta em função da utilização do enlace.

Tratando-se de enlaces Ethernet compartilhados (*half duplex*), o joelho do gráfico encontra-se quando a utilização ainda está em 50%. Neste caso, o aumento da taxa de utilização é também acompanhado pelo aumento da taxa de colisões. Para tecnologias compartilhadas o gráfico é mostrado na Figura 10-6.

Figura 10-6: gráfico de tempo de resposta x utilização de enlace para enlaces de acesso compartilhado.

Em resumo, para enlaces *full duplex* ou de acesso ao meio não compartilhado uma utilização de até 70% é aceitável. Quando se trata de enlaces *half duplex*, utilização maior que 50% já é alarmante.

O modo de operação da interface influencia no cálculo da taxa de utilização. Para interfaces que trabalham no modo *half duplex*, utilize a Equação 10.10-1:

$$\text{Utilização (\%)} = \frac{\text{qtde de bytes recebidos em } \Delta T + \text{qtde de bytes transmitidos em } \Delta T}{\Delta T \text{ x velocidade de operação da interface}} \text{ x 8 x 100}$$

Equação 10.10-1

Quando se trata de interfaces *full duplex*, o cálculo da utilização fica um pouco diferente. Considere, por exemplo, um meio Fast Ethernet operando em modo *full duplex*. Significa que a velocidade do canal é de 100Mbps para transmissão e 100Mbps para recepção, resultando em uma capacidade combinada de 200Mbps.

Existem duas formas de se calcular a utilização de enlaces *full duplex*. Uma delas (Equação 10.10-2) considera apenas uma direção de transmissão: a que estiver com maior tráfego. A forma mais utilizada (Equação 10.10-3 e Equação 10.10-4) separa a taxa de utilização de entrada da taxa de utilização de saída. Veja as equações a seguir:

$$\text{Utilização (\%)} = \frac{\text{max(qtde de bytes recebidos em } \Delta T\text{, qtde de bytes transmitidos em } \Delta T\text{)}}{\Delta T \text{ x velocidade de operação da interface}} \text{ x 8 x 100}$$

Equação 10.10-2

$$\text{Utilização de entrada (\%)} = \frac{\text{qtde de bytes recebidos em } \Delta T}{\Delta T \text{ x velocidade de operação da interface}} \text{ x 8 x 100}$$

Equação 10.10-3

$$\text{Utilização de saída (\%)} = \frac{\text{qtde de bytes transmitidos em } \Delta T}{\Delta T \text{ x velocidade de operação da interface}} \text{ x 8 x 100}$$

Equação 10.10-4

A separação da utilização de entrada e saída também pode ser aplicada a enlaces *half duplex*. Na realidade, é mais freqüente e interessante que a utilização de entrada e saída sejam calculadas separadamente, independentemente do modo de operação do enlace.

Nas seções seguintes você aprenderá como obter os termos das equações apresentadas acima. Substitua-os adequadamente e obterá a taxa de utilização desejada.

10.10.2 Usando uma estação de gerência SNMP

Nesta seção você vai aprender como calcular a utilização de enlaces com o auxílio de uma estação de gerência SNMP. Apresentaremos também que alarmes relacionado à utilização de enlaces podem ser configurados em uma sonda RMON.

Você pode calcular a utilização de seus enlaces com o auxílio dos seguintes objetos do grupo Interfaces da MIB-2 [RFC2233]:

- **ifInOctets** → contador de bytes recebidos por uma interface. Por ser um contador, a diferença entre os valores de **ifInOctets** obtida entre duas coletas consecutivas é que deve ser utilizada no cálculo;

- **ifOutOctets** → contador de bytes que saem de uma interface. Por ser um contador, a diferença entre os valores de **ifOutOctets** obtida entre duas coletas consecutivas é que deve ser utilizada no cálculo;

- **ifSpeed** → a velocidade na qual a interface está operando.

Para realizar o cálculo da utilização você terá que coletar o valor dos objetos **ifInOctets** e **ifOutOctets** em dois momentos distintos. O intervalo de tempo entre as duas coletas de dados SNMP é o ΔT de sua equação.

Por exemplo, suponha que sua estação de gerência SNMP coleta dados de 5 em 5 minutos. Em uma primeira coleta você obteve os seguintes valores:

- **ifInOctets** = 200

- **ifOutOctets** = 3010

- **ifSpeed** = 100000000

Numa segunda coleta os valores dos mesmos objetos (da mesma interface) foram:

- **ifInOctets** = 1225500000

- **ifOutOctets** = 450500000

- **ifSpeed** = 100000000

Você então obtém a utilização de entrada e saída da interface:

$$\text{Utilização de entrada (\%)} = \frac{(1225500000 - 200) \times 8 \times 100}{300 \times 100000000} \approx 32{,}68\%$$

$$\text{Utilização de saída (\%)} = \frac{(450500000 - 3010) \times 8 \times 100}{300 \times 100000000} \approx 12{,}01\%$$

Outros objetos do grupo Interfaces podem também ser utilizados. Eles possuem o mesmo significado dos objetos descritos acima, porém podem atingir valores superiores, pois são representados por contadores de 64 bits, e não 32 bits como os descritos anteriormente. Os objetos são: **ifHCInOctets**, **ifHCOutOctets** e **ifHighSpeed**.

Para interfaces que operam em velocidades inferiores a 20 Mbps os contadores de 32 bits devem ser utilizados. Para interfaces que operam além de 20 Mbps e aquém de 650 Mbps, contadores de quadros de 32 bits e contadores de octetos de 64 bits devem ser utilizados. Para contadores de octetos de 64 bits devem ser utilizados. Finalmente, contadores de 64 bits devem ser utilizados em se

tratando de interfaces que operam além de 650 Mbps. Veja mais informações em [RFC2233], seção “Counter size”.

Com o auxílio de uma sonda RMON pode-se calcular a utilização de um segmento Ethernet mais precisamente, através da Equação 10.10-5 [RFC1757]:

$$\text{Utilização (\%)} = \frac{[\Delta \text{etherStatsPkts x (96 + 64)}] + (\Delta \text{etherStatsOctets x 8})}{\Delta \text{T x velocidade de operação do enlace}} \text{ x 100}$$

Equação 10.10-5

Onde:

- etherStatsPkts é o contador de pacotes recebidos na rede;
- etherStatsOctets é o contador de octetos recebidos na rede;
- entre um quadro e outro existe um intervalo de pelo menos 96 bits e antes de cada quadro existe um preâmbulo de 64 bits. Por isso estes valores são somados e multiplicados pela quantidade de quadros na rede: é quanto se gasta com essas informações de controle.

Se você tem uma sonda RMON monitorando um enlace, configure alarmes que disparem baseados na quantidade de octetos que entram e saem em uma interface. Para os enlaces *full duplex* os dados de cada alarme a ser configurado podem ser os apresentados na Tabela 10-14 e Tabela 10-15.

Variável a ser monitorada:	ifInOctets
Tipo:	deltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	$\frac{\text{velocidade de operação do enlace x 0,7 x 600}}{8}$
Limiar decrescente:	0

Tabela 10-14 Dados para configuração de alarme de utilização de entrada em enlaces full duplex.

Variável a ser monitorada:	ifOutOctets
Tipo:	deltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	$\frac{\text{velocidade de operação do enlace x 0,7 x 600}}{8}$
Limiar decrescente:	Idem limiar crescente

Tabela 10-15: Dados para configuração de alarme de utilização de saída em enlaces full duplex.

Para enlaces *half duplex* configure um alarme com os seguintes dados:

Variável a ser monitorada:	etherStatsOctets

Tipo:	deltaValue
Intervalo:	600 segundos (10 minutos)
Limiar crescente:	$\frac{\text{velocidade de operação do enlace x 0,5 x 600}}{8}$
Limiar decrescente:	Idem limiar crescente

Tabela 10-16: Dados para configuração de alarme de utilização em enlaces half duplex.

Configure estes alarmes para gerar notificações de alarmes (*traps*) para a sua estação de gerência SNMP. Desta forma, sempre que um enlace passar 10 minutos com utilização média superior ao limiar de 70% para enlaces *half duplex* ou 50% para enlaces *half duplex*, sua estação de gerência será avisada.

10.10.3 Usando uma interface de linha de comando

Roteadores e comutadores possuem comandos que informam valores de contadores de bytes de entrada e saída em suas interfaces. Nesta seção apresentaremos alguns comandos que podem ser executados em roteadores/comutadores Cisco com o intuito de obter dados para o cálculo da utilização de enlaces.

Em roteadores Cisco com IOS 10.0 ou superior use o comando a seguir:

```
roteador# show interface [tipo da interface] [número da interface]
```

No exemplo a seguir são obtidas informações sobre a interface Fast Ethernet 1/1/0 de um roteador Cisco:

```
roteador>show inter FastEthernet 1/1/0
    1.  FastEthernet1/1/0 is up, line protocol is up
    2.  Hardware is cyBus FastEthernet Interface, address is 0003.2853.0931
        (bia 0003.2853.0931)
    3.  Internet address is 192.168.4.1/24
    4.  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load
        10/255
    5.  Encapsulation ARPA, loopback not set
    6.  Keepalive set (10 sec)
    7.  Half-duplex, 100Mb/s, 100BaseTX/FX
    8.  ARP type: ARPA, ARP Timeout 04:00:00
    9.  Last input 00:00:00, output 00:00:00, output hang never
    10. Last clearing of "show interface" counters never
    11. Queueing strategy: fifo
    12. Output queue 0/40, 98 drops; input queue 0/75, 0 drops
    13. 5 minute input rate 901000 bits/sec, 566 packets/sec
    14. 5 minute output rate 4104000 bits/sec, 678 packets/sec
    15. 2159137620 packets input, 346328816 bytes, 0 no buffer
    16. Received 1026648 broadcasts, 0 runts, 0 giants, 0 throttles
    17. 0 input errors, 0 CRC, 4 frame, 0 overrun, 0 ignored
    18. 0 watchdog, 0 multicast
    19. 0 input packets with dribble condition detected
    20. 1784610 packets output, 142194201 bytes, 0 underruns
    21. 1664 output errors, 48521009 collisions, 11 interface resets
    22. 0 babbles, 0 late collision, 0 deferred
    23. 1663 lost carrier, 0 no carrier
```

```
24. 0 output buffer failures, 0 output buffers swapped out0
```

Este comando oferece muito mais informações que simplesmente a quantidade de bytes de entrada e saída. Em negrito estão as informações que devem ser buscadas quando se deseja calcular a utilização da interface. As linhas foram numeradas para facilitar a discussão a seguir.

Com a taxa de entrada e de saída da interface e sua velocidade de operação podemos calcular a utilização média de entrada e saída de um enlace para o intervalo de tempo ΔT. O cálculo pode ser feito como apresentado na Equação 10.10-6 e Equação 10.10-7:

$$\text{Utilização de entrada (\%)} = \frac{\text{taxa de entrada de dados}}{\text{Velocidade da interface}} \times 100$$

Equação 10.10-6

$$\text{Utilização de saída (\%)} = \frac{\text{taxa de entrada de dados (bits/s)}}{\text{Velocidade da interface}} \times 100$$

Equação 10.10-7

Nas linhas 13 e 14 são dadas as taxas médias de entrada e saída dos últimos 5 minutos e na linha 7 a velocidade de operação do enlace. Considerando estas informações vamos calcular a utilização de entrada e saída do enlace. Para tal substitua os dados obtidos na Equação 10.10-6 e na Equação 10.10-7. Chegamos às seguintes taxas de utilização de entrada e saída do enlace para os últimos 5 minutos:

$$\text{Utilização de entrada} = \frac{901000 \times 100}{10000000} = 0{,}901\%$$

$$\text{Utilização de saída} = \frac{4104000 \times 100}{100000000} = 4{,}104\%$$

Você pode também obter os valores dos contadores de bytes de entrada e de saída apresentados nas linhas 15 e 20 respectivamente para calcular a taxa de utilização do enlace como apresentado na Equação 10.10-1, Equação 10.10-2 ou Equação 10.10-3 e Equação 10.10-4. Lembre-se que estes dados tratam-se de contadores, e portanto a sua variação em um determinado intervalo de tempo é que deve ser considerada.

Em comutadores Cisco Catalyst com versão de *software* superior a 6.2 os seguintes comandos podem ser executados:

```
show mac [módulo[/porta]]

show mac utilization [módulo[/porta]]

show port mac [modulo[/porta]] (6.2 e superiores)
```

Todos eles oferecem contadores de bytes de entrada e saída. Os dois últimos comandos só existem para comutadores com *software* versão 6.2 ou superiores.

Uma outra informação ainda é necessária para o cálculo da utilização de enlaces: a velocidade de operação da interface. Use o comando a seguir para obter esta informação:

```
show port status [módulo[/porta]]
```

Por exemplo, para obter contadores de tráfego de entrada e saída da porta 1 do módulo 1 execute:

```
Console> show mac utilization 1/1

Console> show port status 1/1
```

Além dos comandos descritos acima, existe ainda um outro comando que oferece todas as informações necessárias para o cálculo da utilização de um enlace:

```
Console> show counters [módulo[/porta]
```

Este comando existe na maioria dos comutadores Cisco. Ele fornece contadores relacionados a uma porta ou todas as portas de um módulo. Muitos contadores são apresentados, dentre eles contadores de octetos de entrada e saída.

Com os dados obtidos através da interface de linha de comando você pode se basear nas equações apresentadas na Seção **DESCRIÇÃO E DICAS** para obter a taxa de utilização de um enlace de um comutador Cisco.

Se seus equipamentos de interconexão não são fabricados pela Cisco, procure no manual do seu equipamento os comandos que lhe oferecem estatísticas de tráfego e velocidade de operação de interfaces.

10.10.4 Usando um analisador de protocolos

Nesta seção veremos como obter a utilização de um enlace com o auxílio de um analisador de protocolos. O primeiro passo é conectar o analisador de forma que ele enxergue apenas os dados da porta cuja utilização você quer medir. Veja UTILIZANDO UM ANALISADOR DE PROTOCOLOS.

Após conectar o analisador, verifique as estatísticas apresentadas por ele. No Sniffer da NAI, um painel com a utilização é apresentado enquanto o enlace é monitorado. Neste mesmo painel você pode escolher ver os detalhes, onde a utilização também é apresentada.

Se você achar que a utilização está muito alta, capture dados durante alguns minutos. Após encerrada a captura, verifique quem foram os dez maiores transmissores (tabela Host Table) durante a captura. Veja também se os dados foram específicos de um determinado serviço (a tabela Matrix pode ser útil).

10.10.5 Usando outras ferramentas de gerência

Esta seção lhe oferece algumas dicas de como obter os dados que são necessários para o cálculo da utilização de enlaces em estações de trabalho que não possuem agente SNMP instalado. Lembre-se: o ideal é que pelo menos nos servidores de sua rede existam agentes SNMP instalados e que a taxa de utilização seja obtida através de uma estação de gerência SNMP.

Em máquinas Linux use o seguinte comando:

```
maria@server:~$ ifconfig eth0
25. eth0      Link encap:Ethernet  HWaddr 00:04:AC:4C:98:DF
26.           inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
27.           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
28.           RX packets:2739527 errors:0 dropped:0 overruns:0 frame:0
29.           TX packets:2240473 errors:0 dropped:0 overruns:0 carrier:0
30.           collisions:0 txqueuelen:100
31.           RX bytes:538341940 (513.4 Mb)  TX bytes:1142036917 (1089.1 Mb)
32.           Interrupt:15 Base address:0x2180
```

Na linha 7 você encontra um contador de bytes de entrada e de saída para a interface. Estes contadores podem ser utilizados no cálculo da taxas de utilização de entrada e saída do enlace.

Você precisa saber também qual a velocidade e o modo de operação da interface. Se você deseja calcular a taxa de utilização de uma interface ligada a uma porta de um comutador ou de um roteador, verifique no comutador/roteador qual o modo e a velocidade de operação da porta em questão (ver página 286). Se a interface está ligada a um repetidor, o modo de operação é *half duplex*. Se a placa de rede é 10 Mbps a velocidade será esta. Se a placa de rede é 10/100Mbps ela provavelmente vai negociar com o outro lado a velocidade. Se o repetidor também é 10/100 Mbps, a velocidade será 100 Mbps. Caso contrário a velocidade será 10 Mbps. Esta análise vale também para máquinas Windows. Mas no Windows, em geral, podemos ver a velocidade e o modo de configuração (se não estiver configurado para negociação automática) nas propriedades avançadas do adaptador de rede instalado.

Em máquinas Windows use o comando a seguir para obter contadores de bytes de entrada e saída em interfaces:

```
C:\WINDOWS>netstat -ne
Estatísticas de interface
                     Recebido      Enviado
Bytes                82161         31128
Pacotes unicast      447           503
Pacotes não unicast  38            38
Descartados          0             0
Erros                0             0
Prot. desconhecidos  48
```

Lembre-se que os valores oferecidos por estes comandos são contadores e, portanto, apenas sua variação no tempo tem algum significado. Obtendo-se a variação destes contadores durante um determinado intervalo de tempo, e

conhecendo a velocidade da interface você pode calcular a taxa de utilização da interface para este intervalo de tempo. Para tal as equações apresentadas na Seção **DESCRIÇÃO E DICAS** devem ser usadas.

10.11 Verificando existência de quadros muito longos

Este procedimento deve ser seguido quando queremos verificar a existência de quadros muito grandes na rede. Na Seção **DESCRIÇÃO E DICAS** explicaremos o que é um quadro muito longo e em que circunstâncias eles podem aparecer na rede. Nas seções seguintes daremos dicas de como verificar a ocorrência de quadros muito longos com o auxílio de uma estação de gerência SNMP, de uma interface de linha de comando e de um analisador de protocolos.

10.11.1 Descrição e Dicas

Quadros Ethernet podem ter um tamanho máximo de 1518 bytes. Quadros maiores que este tamanho são considerados muito longos, ou quadros gigantes.

Tipicamente, quadros muito longos são emitidos por interfaces de rede defeituosas. Quadros muito longos também podem ser enviados ocasionalmente quando um computador é ligado ou reiniciado. Alguns testes em interfaces consistem em preencher o *buffer* da interface com bits 0s ou 1s e em seguida enviar todo o conteúdo do buffer como um quadro longo [GUIA-ETHERNET].

Se vários quadros muito grandes estão sempre presentes na rede uma investigação deve ser realizada, pois a presença contínua destes quadros indica problema. Se alguns poucos quadros muito grandes aparecem esporadicamente, não se preocupe.

10.11.2 Usando uma estação de gerência SNMP

Nesta seção veremos quais objetos SNMP indicam a ocorrência de quadros muito longos na rede. As MIBs Ether-like [RFC2665] e RMON [RFC1757] oferecem objetos que contam a quantidade de quadros muito longos recebidos.

O objeto dot3StatsFrameTooLongs da MIB Ether-like é incrementado sempre que um quadro maior que 1518 bytes é recebido pela interface. Nesta MIB não há separação de quadros muito longos com ou sem erros de CRC ou alinhamento.

Já na MIB RMON, dois objetos indicam o recebimento de quadros muito longos: etherStatsOversizePkts e etherStatsJabbers. O objeto etherStatsOversizePkts é incrementado sempre que um quadro maior que 1518 bytes sem erros de CRC ou alinhamento é recebido pela interface. Já o objeto etherStatsJabbers é incrementado apenas quando um quadro muito longo com erro de CRC ou alinhamento é recebido.

Se os contadores apresentados estiverem crescendo rapidamente, você tem muito provavelmente uma interface defeituosa em sua rede. Um gráfico de quadros muito longos por segundo pode ser gerado pela estação de gerência. Na maior parte do tempo, nenhum quadro longo deve ser encontrado.

10.11.3 Usando uma interface de linha de comando

Nesta seção veremos quais comandos podemos executar em roteadores e comutadores Cisco para verificar a presença de quadros muito longos na rede.

Em roteadores Cisco com versão de IOS superior a 10.0 execute o comando a seguir:

```
show interfaces [tipo da interface] [número da interface]
```

Veja abaixo um exemplo da execução deste comando:

```
roteador> show interface FastEthernet 1/0/0
FastEthernet1/0/0 is up, line protocol is up
(…)
  5 minute input rate 2984000 bits/sec, 916 packets/sec
  5 minute output rate 5099000 bits/sec, 987 packets/sec
     407408230 packets input, 3004139350 bytes, 0 no buffer
     Received 87505 broadcasts, 0 runts, 1 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
(…)
```

Em negrito destacamos o contador que informa a quantidade de quadros maiores que 1518 bytes recebidos pela interface. Se este contador estiver sendo continuamente incrementado uma investigação deve ser iniciada.

Na maioria dos comutadores Cisco execute o seguinte comando:

```
show port [módulo[/porta]]
```

Veja a seguir um exemplo da resposta deste comando:

```
Console> show port 9/5

Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 9/5                     connected           1   auto  auto 10/100BaseTX

(…)

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 9/5           1          2          1          2         2

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts  Giants
----- ---------- ---------- ---------- ---------- --------- ----- -------
 9/5          32          0          0          0         0    30       2

Last-Time-Cleared
--------------------------
Wed Mar 13 2002, 21:57:31
```

O contador de quadros maiores que 1518 bytes recebidos pela interface 9/5 está em destaque (negrito). Verifique se ele está sendo incrementado continuamente.

10.11.4 Usando um analisador de protocolos

Nesta seção veremos como observar a presença de quadros muito longos com o auxílio de um analisador de protocolos.

Conecte o analisador de protocolos como descrito no UTILIZANDO UM ANALISADOR DE PROTOCOLOS. Verifique na tabela de detalhes do painel do Sniffer os contadores intitulados Oversize e Jabber. Estes contadores estão em destaque na Figura 10-7. Se estes contadores estiverem crescendo rápida e continuamente, é provável que exista em sua rede uma ou mais interfaces defeituosas.

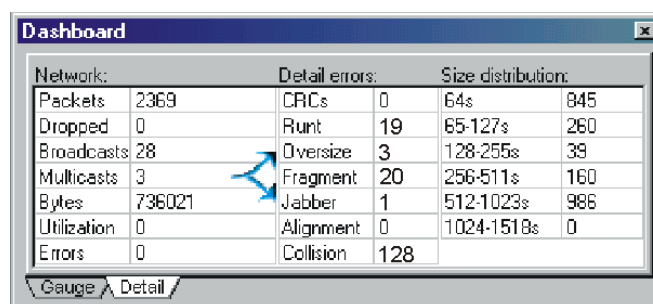



Figura 10-7: Painel de estatísticas detalhadas do Sniffer.

Se você estiver preocupado com a quantidade de quadros muito longos em sua rede, pode usar a funcionalidade de amostragem histórica do Sniffer para analisar esse tráfego. O Sniffer pode gerar para você um gráfico que mostre a quantidade de quadros muito longos por segundo (jabbers/s e oversizes/s) durante um intervalo de tempo de, no máximo, 15 horas. Use este gráfico para analisar melhor a quantidade de quadros muito longos por segundo em sua rede. Se sempre existirem quadros muito longos em sua rede, algum equipamento está com problema.

10.12 Obtendo NEXT e atenuação em cabos de pares trançados

Neste procedimento serão apresentados os conceitos de NEXT (*near end crosstalk*) e atenuação e como verificar se um cabo de pares trançados apresenta NEXT e atenuação fora das especificações do padrão.

10.12.1 Descrição e Dicas

Nesta seção, explicaremos o que é NEXT e atenuação. Na seção seguinte descreveremos que ferramentas utilizar para verificar se um cabo de pares trançados apresenta NEXT e atenuação fora dos limites de padronização do cabo.

Sempre que uma corrente percorre um fio, um campo eletromagnético é gerado. Este campo pode causar interferência com os sinais dos fios adjacentes. Os fios metálicos dos cabos de pares trançados são enrolados entre si (dando a aparência de uma trança) para que os campos eletromagnéticos opostos gerados pela corrente que percorre os fios se cancelem. Quanto mais apertada a trança, mais eficaz será o cancelamento dos campos, e mais altas taxas de dados serão suportadas pelo cabo. Quando os fios não estão bem trançados, o resultado é o NEXT. Em cabos de pares trançados usados em redes locais, NEXT ocorre quando um sinal de um dos pares de fios é apanhado por um par de fios adjacente. NEXT é, então, a porção de sinais transmitidos que é acoplada aos sinais recebidos [CABLETESTING-NEXT].

NEXT é medido em decibéis (dB). Considere $A_{injetado}$ como sendo a amplitude do sinal injetado e $A_{induzido}$ como a amplitude do sinal induzido no par de fios adjacente. Idealmente, queremos que $A_{induzido}$ seja zero. Veja como NEXT é calculado na Equação 10.12-1:

$$\text{NEXT (dB)} = 20 \log \frac{A_{induzido}}{A_{injetado}}$$

Equação 10.12-1

Como $A_{induzido} < A_{injetado}$, o resultado será um número negativo. Note também que quanto menor for o valor de $A_{injetado}$ (menor indução), maior será o módulo do resultado (módulo de NEXT). Assim, queremos que o valor do NEXT seja muitos decibéis (negativos), o que significa muita perda entre um par e outro (ou pouco acoplamento).

Todos os sinais eletromagnéticos perdem um pouco de sua força à medida que se propagam pelo meio. Por esta razão, os sinais que se propagam de uma extremidade a outra de um cabo de pares trançados chegam na extremidade final com um pouco menos de força. A atenuação é justamente a perda de potência que o sinal sofre ao longo do caminho entre o transmissor e o receptor. Quanto mais forte a atenuação, mais fraco será o sinal na extremidade receptora.

A atenuação, assim como o NEXT, é medida em decibéis (dB). Como a atenuação significa uma perda, ela é expressa sempre por valores negativos. Quanto menor a perda melhor.

Considere $A_{entrada}$ como sendo a amplitude do sinal injetado no início do cabo e $A_{saída}$ a amplitude do sinal na saída. Idealmente queremos que $A_{saída}$ seja igual a $A_{entrada}$, o que significa que ao houve atenuação. Veja como a atenuação é calculada na Equação 10.12-2:

$$\text{Atenuação (dB)} = 20 \log \frac{A_{saída}}{A_{entrada}}$$

Equação 10.12-2

Se $A_{saída} = A_{entrada}$, teríamos atenuação zero, pois log 1 = 0. Como, na prática, $A_{saída} < A_{entrada}$, o resultado será um número negativo. Note que quanto menor

for a diferença $A_{saída} - A_{entrada}$ (pouca atenuação) mais próximo de zero estará a atenuação. Assim, queremos que o valor da atenuação próximo de zero (poucos decibéis negativos), o que significa pouca perda.

10.12.2 Usando uma ferramenta de certificação

Existem vários tipos de ferramentas usadas para testar cabos de redes. Estas ferramentas recaem em quatro grandes classes: analisadores de rede, ferramentas portáteis de certificação, testadores de cabos e testadores de continuidade. Destas, apenas analisadores de rede e ferramentas de certificação são capazes de medir NEXT e atenuação [FIELD_TEST].

Analisadores de rede são equipamentos caros e requerem uma equipe técnica altamente treinada para lidar com eles. São ferramentas geralmente utilizadas em laboratórios para avaliar o desempenho de cabos em desenvolvimento [FIELD_TEST]. Por esta razão, não falaremos neste procedimento sobre esse tipo de equipamento.

Ferramentas portáteis de certificação, por outro lado, podem ser utilizadas por usuários menos sofisticados. Elas são tipicamente utilizadas para verificar se uma infra-estrutura de cabeamento atende aos requisitos impostos pelos padrões de cabeamento [FIELD_TEST]. Exemplos de equipamentos de certificação são o OmniScanner e PentaScanner da Microtest e os DSP séries 2000 e 4000 da Fluke.

Recomenda-se que o NEXT seja medido nas duas extremidades de um cabo, principalmente quando se tratam de cabos mais compridos. Se um cabo possui uma terminação mal feita em uma extremidade, ao testar o cabo a partir da extremidade oposta, mesmo que o NEXT esteja fora do padrão, é possível que o cabo passe no teste devido à atenuação sofrida pelo sinal [FLUKE-NET-NEXT].

Para cada categoria de cabo existem valores limites de NEXT e atenuação. As próprias ferramentas de certificação irão testar seu cabo e apresentar um relatório que informa se ele está ou não de acordo com as especificações do padrão do cabo em teste. Em outras palavras, você não precisa decorar qual o valor máximo aceitável em decibéis da atenuação ou do NEXT em um cabo de pares trançados categoria 5. O próprio testador vai lhe dizer se seu cabo está ou não de acordo com o padrão.

Para que o seu teste seja válido você precisa apenas informar ao testador qual a categoria do cabo que vai ser testado. Suponha que você deseja testar um cabo de pares trançados categoria 5. Mas, acabou selecionando no testador a categoria 5E. É bem possível que o teste falhe, pois cabos de categoria 5 têm requisitos de desempenho aquém dos cabos de categoria 5E.

A Tabela 10-17 [SIEMON] oferece NEXT e atenuação de cabos categorias 5, 5e, 6 e 7 a 100 MHz. Ela mostra ainda valores de NEXT e atenuação para cabos categorias 6 e 7 a 250 MHz e 600 MHz. Os limiares apresentados correspondem aos piores casos. Tipicamente, encontraremos valores de atenuação e NEXT melhores que os apresentados.

Não entraremos em mais detalhes sobre como usar uma ferramenta de certificação por ser uma tarefa bastante dependente do modelo e fabricante da ferramenta. Leia nos manuais do seu equipamento como proceder.

	Categoria 5 (100 MHz)	Categoria 5e (100 MHz)	Categoria 6 (100 MHz/250 MHz)	Categoria 7 (100 MHz/600 MHz)
NEXT	27.1 dB	30.1 dB	39.9 dB/33.1 dB	62.1 dB/51 dB
Atenuação	24 dB	24 dB	21.7 dB/ 36 dB	20.8 dB/ 54.1 dB

Tabela 10-17: Valores limites de atenuação e NEXT em cabos de pares trançados categorias 5, 5e, 6 e 7.

10.13 Obtendo estado administrativo de interfaces

Neste procedimento descreveremos como obter o estado administrativo de interfaces de equipamentos de interconexão e estações de trabalho.

10.13.1 Descrição e Dicas

É possível que interfaces de equipamentos de interconexão não mais transmitam dados devido a defeitos físicos. No entanto, é possível também que uma interface pare de receber e enviar quadros por ordem do administrador da rede. Quando o gerente de rede desativa uma interface diz-se que ela está administrativamente desabilitada. Isto quer dizer que o gerente da rede pode habilitar ou desabilitar uma interface administrativamente de acordo com os requisitos de gerência de sua rede.

Por exemplo, considere um comutador que fica no laboratório de usuários. Algumas portas do comutador estão vazias. A política de segurança da empresa dita que não é permitido que máquinas novas sejam inseridas na rede sem que a equipe de gerência da rede seja consultada. Para auxiliar o cumprimento desta regra da política de segurança, você pode desabilitar administrativamente as portas vagas do comutador, assim, elas não serão facilmente utilizadas para a conexão de novas máquinas.

Você vai desejar verificar o estado administrativo de uma interface em algumas situações. Por exemplo:

- você está conectando uma nova máquina na rede ou recebeu reclamações de usuários de que a rede não está funcionando. A interface à qual a nova máquina ou a máquina do usuários está ligada pode estar administrativamente desabilitada (problema INTERFACE DESABILITADA);

- você quer encontrar falhas na rede. Se uma interface está inativa porque o gerente assim o deseja, tudo bem. No entanto, quando o estado operacional de uma interface está diferente do estado administrativo, uma investigação deve ser iniciada. Encontrar uma interface não operacional cujo estado administrativo indica que ela deveria estar ativa é uma indicação de falha na interface.

Nas seções a seguir você aprenderá como obter o estado administrativo de uma interface.

10.13.2 Usando uma estação de gerência SNMP

Nesta seção será apresentado como obter o estado administrativo de uma interface usando uma estação de gerência SNMP.

A variável de gerência ifAdminStatus do grupo Interfaces da MIB-2 [RFC 2233] informa o estado administrativo de uma interface. Esta variável tem um valor inteiro entre 1 e 3:

- 1 indica interface ativa;
- 2 indica interface inativa;
- 3 indica que a interface está em teste.

Se você deseja comparar o estado administrativo de uma interface com o operacional, será necessário recuperar também o valor de outra variável de gerência da mesma MIB: ifOperStatus. Veja o **OBTENDO ESTADO OPERACIONAL DE INTERFACES**.

10.13.3 Usando uma interface de linha de comando

Nesta seção mostramos como verificar o estado administrativos de interfaces de comutadores e roteadores Cisco usando uma interface de linha de comando.

Na maioria dos roteadores Cisco todos os comandos seguintes podem ser executados para obter o estado das interfaces do roteador:

```
roteador# show inter accounting
roteador# show interfaces
roteador# show inter description
```

Se preferir, você pode selecionar apenas uma interface. Por exemplo, em roteadores Cisco família 7500, execute:

```
roteador# show interface [tipo_da_interface] [número_da_interface]
```

Este comando apresentará informações sobre a interface selecionada. Por exemplo, para obter informações sobre a interface FastEthernet 1/0/0 o seguinte comando deve ser executado:

```
#show interface FastEthernet 1/0/0
```

A primeira linha de retorno indica o estado administrativo da interface. Se ela estiver habilitada e funcionando a primeira linha será a seguinte:

```
FastEthernet1/1/0 is up, line protocol is up
```

Caso a interface esteja administrativamente desativada, a primeira linha será:

```
FastEthernet1/1/0 is administratively down, line protocol is
down
```

O comando a seguir informa o estado das portas na maioria dos comutadores Cisco Catalyst (a partir da família 29xx):

```
comutador> show port status [módulo[/porta]]
```

Veja o exemplo a seguir:

```
Console> show port status
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------
---
1/1                     disabled   1          normal   half  100
100BaseTX
1/2                     notconnect 1          normal   half  100
100BaseTX
2/1                     connected  trunk      normal   half  400
100BaseTX
3/1                     notconnect trunk      normal   full  155 OC3 MMF
ATM
5/1                     notconnect 1          normal   half  100
100BaseTX
5/2                     notconnect 1          normal   half  100
100BaseTX
```

Em comutadores Cisco, o estado `disabled` indica que a porta está desabilitada. A porta 1/1 do exemplo apresentado está inativa administrativamente. Existem outros estados. O estado `notconnect`, por exemplo, indica que a interface está habilitada, mas não foi possível estabelecer conexão com o lado remoto (o equipamento remoto está desligado, por exemplo).

Se você possui outros modelos ou marcas de comutadores/roteadores, descubra como verificar o estado administrativo das portas nos manuais de comandos ou de configuração do seu equipamento. Em geral, não será uma atividade muito complexa.

10.13.4 Usando ifconfig

Nesta seção veremos como obter o estado administrativo de interfaces em máquinas Linux e Windows.

Em máquinas Linux o comando `ifconfig -a` pode ser utilizado. Ele retornará uma lista completa com todas as interfaces da máquina, inclusive as que estão desabilitadas. Um exemplo do retorno deste comando é:

```
root# ifconfig –a
```

```
eth0 Link encap:Ethernet  HWaddr 00:60:94:63:6E:3A
     inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:658685 errors:0 dropped:0 overruns:0 frame:3
     TX packets:555222 errors:0 dropped:0 overruns:19 carrier:1
     collisions:44644 txqueuelen:100
     Interrupt:5

eth1 Link encap:Ethernet  HWaddr 00:60:94:63:6E:3A
     inet addr:10.10.12.1  Bcast:10.10.12.255  Mask:255.255.255.0
     BROADCAST MULTICAST  MTU:1500  Metric:1
     RX packets:85 errors:0 dropped:0 overruns:0 frame:0
     TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
     collisions:4 txqueuelen:100
     Interrupt:10
(…)
```

No exemplo dado a interface eth0 está habilitada. Note que ela está "UP" e "RUNNING". Já eth1 não está. Tipicamente, quando uma interface está administrativamente desabilitada ela é apresentada pelo comando `ifconfig -a` como a interface eth1: não apresentando os *flags* "UP" e "RUNNING".

O comando `ifconfig` é usado para ativar e desativar interfaces administrativamente. É provável que a interface eth1 do exemplo dado tenha sido desativada pelo comando:

```
root# ifconfig eth1 down
```

Quando desabilitamos uma interface administrativamente, as rotas que a utilizam são automaticamente desativadas. Caso a tabela de rotas seja configurada estaticamente, ao ativar a interface manualmente será necessário também inserir as rotas que foram desativadas.

Para ativá-la novamente use o comando:

```
root# ifconfig eth1 up
```

Se a placa de rede eth1 não estiver com defeito e seu *driver* estiver corretamente instalado, após sua ativação eth1 apresentará os flags "UP" e "RUNNING" assim como eth0 e estará apta a receber e enviar dados.

Em máquinas Windows interfaces podem ser administrativamente desativadas através do Gerenciador de Dispositivos. No Windows 2000 você pode verificar o estado administrativo de uma interface seguindo os passos a seguir:

- clique com o botão direito do mouse sobre o ícone Meu Computador. No menu que surgir escolha o item Propriedades;
- na tabela Hardware, pressione o botão Gerenciador de Dispositivos;
- clique com botão direito do mouse sobre a placa de rede cujo estado você deseja verificar;

- no menu que surgir escolha o item Propriedades. Uma janela apresentando as propriedades da placa de rede selecionada aparecerá;
- nesta janela é possível verificar se a placa de rede está ou não habilitada. É possível também modificar o estado da placa, se desejado.

10.14 Verificando ocorrência de enchentes

Neste procedimento descreveremos como verificar se comutadores estão enviando muitos quadros em enchente.

10.14.1 Descrição e Dicas

Comutadores mantêm tabelas de endereços, que informam através de qual interface um certo endereço MAC pode ser alcançado. Estas tabelas iniciam-se vazias, e à medida que as máquinas se comunicam através do comutador, elas vão sendo povoadas, através de uma técnica conhecida por *backward learning*. Ao receber um quadro através de uma de suas portas, emitido por uma máquina origem A, o comutador aprende através de que porta a máquina A pode ser alcançada, e adiciona esta informação na sua tabela. Ao receber um quadro destinado a um certo endereço físico, o comutador procura em sua tabela de endereços através de que porta o quadro deve ser enviado. Se não encontrar esta informação na tabela de endereços, o quadro é enviado para todas as portas do comutador, exceto a porta pela qual o quadro foi recebido. Chamamos este envio de um quadro para todas as portas do comutador de *flooding*, que traduzimos aqui como enchente.

A ocorrência muito freqüente de enchentes é um dos sinais do problema TEMPO DE ENVELHECIMENTO DE TABELAS DE ENDEREÇOS INADEQUADO, apresentado na página 94.

10.14.2 Usando uma estação de gerência SNMP

Utilizando uma estação de gerência SNMP podemos recuperar o valor do tempo de envelhecimento de entradas de tabelas de endereços em comutadores. Mas, não será possível analisar as enchentes. Nesta seção indicaremos que objetos SNMP oferecem informações sobre tabelas de endereços de comutadores.

O objeto dot1dTpAgingTime da Bridge MIB [RFC1493] indica por quanto tempo informações da tabela de endereços aprendidas dinamicamente são válidas. Outro objeto interessante desta mesma MIB – o dot1dTpLearnedEntryDiscards – indica quantas vezes uma entrada da tabela de endereços que acabou de ser aprendida teve que ser descartada por não haver mais espaço suficiente para armazená-la.

Se dot1dTpAgingTime for muito pequeno, enchentes freqüentes ocorrerão, já que o comutador armazenará entradas na tabela de endereços durante pouco

tempo e logo não saberá mais para que porta enviar um quadro destinado a um certo endereço MAC. Se existem tantas entradas na tabela de endereços que não há mais espaço para o armazenamento de novas entradas (dot1dTpLearnedEntryDiscards cresce continuamente), o comutador também poderá ter que enviar muitos quadros em enchente.

Estes objetos nos dão informações importantes sobre a tabela de endereços de um comutador. Mas, apenas na seção a seguir, com o auxílio de um analisador de protocolos, podemos verificar e analisar a ocorrência de enchentes.

10.14.3 Usando um analisador de protocolos

Nesta seção descreveremos como um analisador de protocolos pode nos auxiliar a verificar a ocorrência de enchentes e analisá-la. Na realidade, precisaremos de dois analisadores de protocolos, não apenas de um.

Conecte os analisadores no comutador a ser analisado. Capture quadros em ambos os analisadores durante alguns minutos. É aconselhável que a captura e o encerramento dela sejam simultâneos em ambos os analisadores.

Após encerrar a captura, compare os quadros capturados pelos analisadores. Você verificará que muitos quadros – apesar de não serem destinados a endereços de difusão – foram capturados por ambos os analisadores. Isto significa que o comutador não sabia para que porta enviá-los e eles foram transmitidos por enchente.

Aconselhamos anteriormente que o início e o término da captura fossem simultâneos para facilitar a análise dos quadros capturados. Os analisadores de protocolos geralmente informam o tempo real de captura do quadro – 15 de março de 2002, 15:17:10, por exemplo – e o tempo relativo, considerando que a captura iniciou no tempo 00:00:00.000. O tempo relativo de captura dos quadros pode ajudar a descobrir quadros enviados por enchentes. Eles são enviados no mesmo período após o início da captura.

Verifique o endereço MAC destino dos quadros transmitidos através de enchentes. Se quadros com o mesmo endereço MAC destino foram transmitidos através de enchente em curtos espaços de tempo – menos de 5 minutos – é bastante provável que o tempo de envelhecimento das entradas da tabela de endereços esteja inadequado. Apesar de muito raro, é possível ainda que a tabela de endereços esteja muito grande, e não exista mais espaço no comutador para armazenar novas entradas, tornando a tabela incompleta. Um comutador Cisco Catalyst, por exemplo, tem memória suficiente para armazenar 16 mil entradas nesta tabela. Portanto, esta realmente não será uma situação comum. É preciso estar lidando com equipamentos com menor capacidade de armazenamento para que ela possa vir a ocorrer.

10.15 Analisando tráfego de difusão ARP

Neste procedimento apresentaremos como analisar solicitações ARP em um domínio de difusão.

10.15.1 Descrição e Dicas

O protocolo ARP é utilizado para mapear endereços IP (lógicos) em endereços MAC (físicos). O protocolo ARP, resumidamente, funciona da seguinte forma: quando uma máquina não sabe o endereço MAC correspondente a um certo IP, ela envia um quadro de difusão na rede solicitando à máquina com o endereço IP em questão que informe seu endereço MAC.

Tipicamente, uma máquina não fará mais que 1 consulta ARP a cada 10 segundos. Se em um domínio de difusão existirem N máquinas, não devemos encontrar neste domínio mais que N/10 solicitações ARP por segundo. Na prática, o número de solicitações ARP é bem menor. Mesmo que todos os usuários das N máquinas estivessem utilizando serviços que requeiram muitos mapeamentos IP → MAC, é praticamente impossível que todos eles façam uma solicitação a cada segundo. Em geral encontraremos um número bem menor que N.

Dentre as causas do aumento do tráfego de difusão ARP encontram-se:

- o tempo de validade da *cache* ARP em estações de trabalho, roteadores e comutadores da rede está muito pequeno (ver problema VALIDADE DA CACHE ARP INADEQUADA);
- sua rede está sendo alvo de ataques.

10.15.2 Usando um analisador de protocolos

Nesta seção veremos como analisar o tráfego de difusão ARP em um domínio de difusão usando um analisador de protocolos.

Um analisador de protocolos é a ferramenta mais apropriada para a análise do tráfego ARP em um domínio de difusão. Conecte o analisador em um comutador ou repetidor que faça parte do domínio de difusão que você deseja analisar.

O primeiro passo é criar um filtro, que capture apenas os quadros que carreguem solicitações de mapeamento ARP. Se quiser capturar apenas as requisições ARP, adicione também uma regra que selecione apenas quadros ARP cujo endereço destino é o de difusão (físico). Dicas para a criação deste filtro são encontradas na página 222.

Selecione o filtro de captura ARP que acabou de ser criado e inicie a captura. Capture algumas dezenas de quadros. Após a captura podemos realizar algumas análises:

- quantas requisições ARP por segundo você capturou? Isso pode ser feito olhando as estatísticas de captura. A tabela de estatísticas de captura é mostrada na Figura 10-8. Note que durante 36 segundos capturamos 1230 quadros de requisição ARP. Isto nos dá uma média de 34 requisições ARP por segundo. Este número está muito grande? Existem mais de 34 máquinas no domínio de difusão?

- qual é o endereço IP de quem envia os quadros de solicitação de mapeamento ARP? Se muitos quadros de requisições ARP estão trafegando na rede, observe quem solicita estes mapeamentos ARP. A Figura 10-9 apresenta a decodificação de um quadro de requisição ARP. O endereço da máquina que está enviando a solicitação ARP é indicado no Sniffer pelo rótulo Sender's protocol address. Podemos listar pelo menos duas situações de erros bem definidas:

- se for o roteador de acesso à sub-rede sob estudo que está requisitando os mapeamentos ARP, significa que existem máquinas em outras sub-redes que desejam falar com as máquinas desta sub-rede. Se o roteador solicita o mapeamento do mesmo IP em curtos espaços de tempo, verifique a validade da cache ARP deste roteador. Se o roteador solicita mapeamentos IP ⇒ MAC de endereços IP que não estão alocados a máquina alguma, desconfie de ataques. Em 2002 todo o mundo sofreu com ataques de vermes. O Code Red [CODERED] e o Nimda [NIMDA] foram os mais poderosos. Quando colocávamos o Sniffer para capturar requisições ARP percebíamos que o roteador solicitava mapeamentos de IPs que não estavam alocados a máquina nenhuma. Foi quando começamos a desconfiar de ataques. Mais tarde recebemos a informação do CERT (*Computer Emergency Response Team*) sobre o Code Red;

- se os endereços de quem solicita os mapeamentos ARP não fazem parte da sub-rede em estudo, desconfie de problemas com VLANs. Em geral máquinas de uma mesma rede IP compartilham o mesmo domínio de difusão. Suponha que as máquinas do domínio de difusão sob análise possuem endereços da rede 192.168.1.0/24. Não seria estranho que uma máquina cujo endereço IP é da rede 192.168.3.0/24 solicitasse mapeamentos ARP no domínio de difusão sob estudo? Isto é um sinal típico de problemas com VLANs – máquina inserida na VLAN incorreta (ver página 130). É possível também que existam máquinas com endereços IP incorretos;

- as solicitações ARP pedem o mapeamento de quais endereços IP? Estes endereços existem? Eles fazem parte da classe de endereços da sub-rede em estudo? Na Figura 10-9 o endereço IP que deve ser mapeado está selecionado.

- se o endereço IP existe na sub-rede e o mapeamento for possível, tudo bem. Mas se o endereço não existir suspeite de ataques, como já falamos anteriormente;

- se o endereço pertence a outra sub-rede, podem existir máquinas com configurações de rede incorretas. Por exemplo, suponha que a máquina 192.168.1.1 solicitou o mapeamento IP ⇒ MAC do endereço IP 192.168.3.2. Não é estranho? A máquina 192.168.1.1 acha que pode fazer uma entrega direta à máquina 192.168.3.2, que pertence a outra sub-rede e a outro domínio de difusão. Suspeite da configuração de rede das máquinas que solicitam mapeamentos ARP de endereços IP de outras sub-redes.

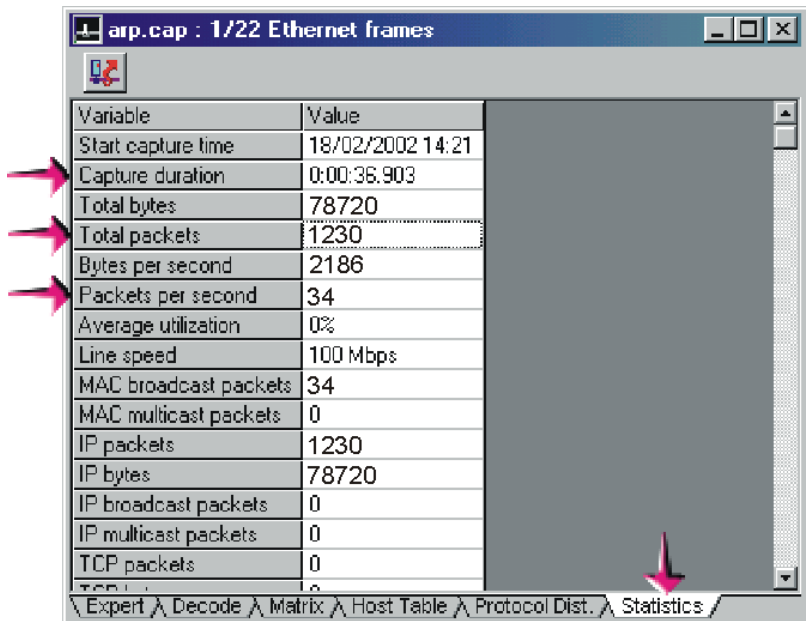



Figura 10-8: Tabela de estatísticas de captura.

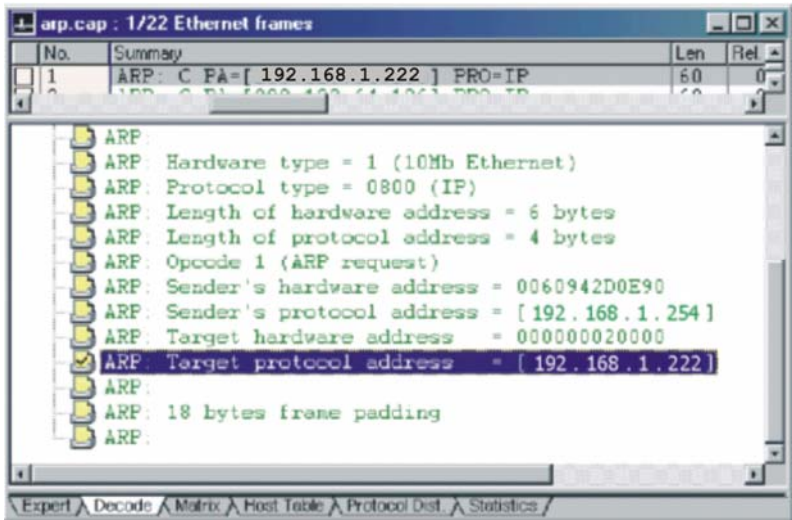



Figura 10-9: Quadro de solicitação ARP.

10.16 Referências

10.16.1 Livros

[DESIGNING-CISCO] Teare, D. Designing Cisco Networks. Cisco Press. Fevereiro, 1999.

[GUIA-ETHERNET] Spurgeon, C. E. Ethernet – O Guia Definitivo. Tradução Daniel Vieira, Editora Campus, 2000.

[HAUGDAHL] Haugdahl, J. Scott. Network Analysis and

Troubleshooting. Addison Wesley, 2000

[PERF&FAULT-CISCO] Maggiora, P. L. D., Elliot, C. E., Pavone Jr, R. L., Phelps, K. J., Thompson, J. M. Performance and Fault Management. Cisco Press. 2000.

10.16.2 Recursos online (Internet)

[CABLETESTING-NEXT] Near End Crosstalk (NEXT).

http://www.cabletesting.com/CableTesting/Testing/Definitions/Definitions_NEXT.htm

[CISCO-MEMORY-POOL-MIB] Johnson, J., Wang, S. CISCO-MEMORY-POOL-MIB. Julho, 2001.

ftp://ftp.cisco.com/pub/mibs/v1/CISCO-MEMORY-POOL-MIB-V1SMI.my

[CISCO-PERF-BP] Cisco Performance Management: Best Practices White Paper.

http://www.cisco.com/warp/public/126/perfmgmt.htm

[CISCO-SPAN] Configuring the Catalyst Switched Port Analyzer (SPAN) Feature.

http://www.cisco.com/warp/public/473/41.html

[CODERED] Informações do CERT sobre o verme Code Red I.

http://www.cert.org/incident_notes/IN-2001-08.html

[FIELD_TEST] An up-to-date review of physical layer measurements, cabling standards, troubleshooting practices and certification techniques.

http://www.wwtc.edu/nsf/AAMI_San_Jose/Arne_WebSite/cabling/cableTestingHandbook.pdf

[FLUKE-NET-NEXT] NEXT.

http://www.fluke-net.com/consultants/testing/next.asp

[NIMDA] Informações do CERT sobre o verme NIMDA.

http://www.cert.org/advisories/CA-2001-

26.html

[OLD-CISCO-MEMORY-MIB] Johnson, J., Wang, S. OLD-CISCO-MEMORY-MIB. Fevereiro, 1994.

ftp://ftp.cisco.com/pub/mibs/v1/OLD-CISCO-MEMORY-MIB.my

[SIEMON] Rybinski, V. De-Mystifying Category 5, 5e, 6, and 7 Performance Specifications. Dezembro, 1999.

http://www.siemon.com/white_papers/99-12-17-demystifying.asp

[CISCO-PROCESS-MIB] CISCO-PROCESS-MIB Definitions.

ftp://ftp.cisco.com/pub/mibs/v1/CISCO-PROCESS-MIB-V1SMI.my

[CPU-UTILIZATION-HOWTO] How to Collect CPU Utilization on Cisco IOS Devices Using SNMP.

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a94.shtml

[OLD-CISCO-SYSTEM-MIB] Jeffrey, J. T. Cisco System MIB file. Julho de 1994.

ftp://ftp.cisco.com/pub/mibs/v1/OLD-CISCO-SYS-MIB.my

10.16.3 RFCs

[RFC1213] McCloghrie, K., Rose, M. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Março, 1991.

[RFC1514] Grillo, P., Waldbusser, S. Host Resources MIB. Setembro, 1993.

[RFC1757] Waldbusser, S. Remote Network Monitoring Management Information Base. Fevereiro, 1995.

[RFC2233] McCloghrie, K., F. Kastenholz. The Interfaces Group MIB

using SMIv2. Novembro, 1997.

[RFC2358] Flick, J., Johnson, J. Definitions of Managed Objects for the Ethernet-like Interface Types. Junho, 1998.

[RFC2665] Flick, J., Johnson, J. Definitions of Managed Objects for the Ethernet-like Interface Types. Agosto de 1999.

[RFC1493] Decker, E., Langille, P., Rijsinghani, A., McCloghrie, K. Definitions of Managed Objects for Bridges. Julho, 1993

11 Procedimentos referenciados nos problemas de nível de rede

Neste capítulo apresentamos 14 procedimentos que informam como obter e analisar informações de gerência. Os procedimentos apresentados neste capítulo informam como obter os sinais que foram mais referenciados nos problemas de nível de rede. No entanto, existem alguns problemas de outras camadas que podem lhes referenciar.

11.1 Verificando se duas máquinas respondem à mesma consulta ARP

Neste procedimento mostraremos como verificar se mais de uma interface está respondendo a uma mesma consulta ARP.

11.1.1 Descrição e Dicas

O protocolo ARP é usado para mapear endereços IP em endereços físicos (MAC). Quando uma estação deseja descobrir o endereço MAC da máquina que possui um determinado endereço IP, ela envia um quadro de difusão solicitando à máquina configurada com este endereço IP que informe o seu endereço MAC. Quando duas ou mais estações respondem à mesma requisição ARP, duas ou mais estações estão configuradas com o mesmo endereço IP.

É usando este raciocínio que os sistemas operacionais de rede da Microsoft se protegem contra endereços duplicados. Antes de usar um endereço de rede uma máquina certifica-se de que ele não está duplicado, enviando uma consulta ARP envolvendo este endereço. Se alguma outra máquina da rede estiver configurada para usar o mesmo endereço IP, ela responderá à consulta ARP. A máquina que realizou o teste terá sua placa de rede desabilitada – o usuário será informado disso – para que não existam endereços IP duplicados na rede.

11.1.2 Usando um analisador de protocolos

Neste procedimento mostraremos como podemos usar um analisador de protocolos para verificar se mais de uma máquina da rede responde a uma mesma consulta ARP, isto é, se existem endereços IP duplicados na rede.

Como sempre, o primeiro passo é conectar o analisador de protocolos no local apropriado. Precisamos capturar, além de consultas ARP, as respostas correspondentes. As consultas ARP são destinadas ao endereço de difusão, portanto, todas as máquinas que fazem parte do mesmo domínio de difusão as recebem. Já as respostas são destinadas apenas à máquina que enviou a consulta correspondente. Daremos aqui duas opções:

- se todas as máquinas da rede em estudo estão conectadas entre si por repetidores, conecte o analisador em um dos repetidores e proceda como descrito no Teste A;

- se existem máquinas ligadas a comutadores, conecte o analisador em um comutador ou em um repetidor (o equipamento que estiver conectado a mais máquinas do domínio de difusão) e proceda como descrito no Teste B. Se você ligar o analisador em um comutador, lembre-se que ele deve fazer parte da VLAN que define o domínio de difusão sob análise;

TESTE A

Como todas as máquinas do domínio de difusão estão ligadas em repetidores, o analisador enxergará todas as consultas e respostas ARP que trafegam neste domínio de difusão. Selecione um filtro que capture apenas quadros contendo dados do protocolo ARP. Capture algumas dezenas de quadros. Ao encerrar a captura, analise os quadros capturados em busca de duas respostas à mesma consulta ARP. Este procedimento não garante que endereços duplicados não existam na sua rede. Você só verá duas respostas ARP à mesma consulta caso tenha a sorte de, durante a captura, alguma máquina realizar uma consulta ARP envolvendo endereços IP duplicados. Este é um teste mais simples, porém menos conclusivo que o Teste B. Portanto, se preferir, realize o procedimento descrito no Teste B.

TESTE B

Ao contrário do procedimento descrito no Teste A, não ficaremos aqui à mercê da sorte. Em contrapartida, este será um processo um pouco mais trabalhoso. Nós mesmos enviaremos consultas ARP na rede. Se você suspeita que algum IP está duplicado, inicie o processo testando este IP. Primeiramente, configure o seu analisador com um endereço IP e máscara de rede que permitam-no se comunicar com outras máquinas da rede. O segundo passo é certificar-se (usando o comando `arp` em sistemas Linux e Windows) de que a tabela ARP de seu equipamento está vazia. No Windows e no Linux, cada entrada precisa ser removida individualmente. Em ambos os sistemas operacionais mencionados o comando a seguir pode ser usado para cada um dos endereços a serem removidos da tabela.

```
C:\WINDOWS> arp –d <endereço IP da entrada a ser removida>
```

```
# arp –d <endereço IP da entrada a ser removida>
```

Em um roteador Cisco com IOS versão 10.0 ou superior, o comando a seguir apagará todas as entradas da tabela ARP:

```
roteador# clear arp-cache
```

Para causar o envio de uma consulta ARP envolvendo um determinado endereço IP da mesma sub-rede, envie mensagens ICMP Echo (`ping`) para este endereço IP. Para que esta mensagem seja enviada, será necessário fazer antes o

mapeamento IP ⇒ MAC. Desta forma, nos podemos induzir o envio de consultas ARP envolvendo o endereço IP que desejarmos. Seu analisador capturará as consultas e as respostas, já que estas serão endereçadas a ele.

Selecione o filtro que capture apenas quadros do protocolo ARP e inicie a captura. Durante a captura, force o envio de consultas ARP para os endereços IP que você desejar usando `ping`. Ao encerrar a captura, analise os quadros capturados em busca de duas respostas à mesma consulta ARP.

11.2 Verificando ocorrência de consultas ARP sem resposta

Neste procedimento mostraremos como verificar a existência de consultas ARP sem resposta em uma rede.

11.2.1 Descrição e Dicas

O protocolo ARP é usado para fazer mapeamentos IP → MAC em uma rede. Quando uma máquina deseja descobrir o endereço MAC correspondente a um determinado endereço IP, ela envia uma consulta ARP em difusão na rede. A máquina que está usando o endereço IP em questão responde esta consulta, informando o seu endereço MAC.

Consultas ARP sem resposta podem simplesmente indicar que a máquina cujo endereço MAC deseja-se descobrir está desligada. Porém, podem também indicar problemas tais como máscara de rede incorreta, equipamentos inseridos na VLAN incorreta e falta de troca de informações sobre VLANs entre comutadores. Estes problemas são apresentados nas Seções 6.3, 6.7 e 6.9, respectivamente.

Além disso, consultas ARP sem resposta podem também indicar que o endereço IP a ser mapeado não está alocado a máquina alguma na rede. Em geral, esta é uma situação causada por ataques. O código malicioso gera endereços aleatórios, que podem ou não existir.

11.2.2 Usando um analisador de protocolos

Veremos nesta seção como usar um analisador de protocolos para checar a existência de consultas ARP sem resposta em um domínio de difusão.

O primeiro passo é conectar o analisador de forma que ele capture consultas e respostas ARP. Se no domínio de colisões em estudo existem apenas repetidores, simplesmente conecte o analisador em um dos repetidores.

Quando existem comutadores no domínio de difusão, a conexão do analisador torna-se um pouco mais trabalhosa. As consultas ARP serão sempre capturadas, pois elas são direcionadas ao endereço de difusão. Já as respostas a estas consultas – que precisamos analisar – são endereçadas à máquina que realizou a consulta. Por isto, se existem comutadores no domínio de difusão não poderemos ver todas as respostas ARP.

Se existe apenas um comutador, você pode optar por espelhar todas as portas do comutador que participam do domínio de difusão (mesma VLAN) em questão em uma outra porta, e conectar nesta porta o analisador de protocolos. No entanto, nem todos os comutadores permitirão que isso seja feito. Além disso, essa solução só será possível se o tráfego combinado de cada porta espelhada não ultrapassar a banda passante da interface na qual os dados forem espelhados. Uma outra alternativa é conectar os equipamentos conectados no comutador que participam do domínio de difusão em estudo em um repetidor e conectar este repetidor no comutador. Conecte o analisador de protocolos neste repetidor. Da mesma forma, deve-se tomar cuidado para não saturar a largura de banda dos enlaces do repetidor.

Se no domínio de difusão em estudo existe mais de um comutador, o analisador pode ser conectado da mesma forma descrita acima (quando existe apenas um comutador), mas nesta situação, o analisador capturará apenas as respostas ARP destinadas a equipamentos ligados ao mesmo comutador ao qual o analisador está conectado. procedimento será um pouco diferente. Mais adiante, abordaremos esta situação.

Se o analisador de protocolos foi conectado de forma que requisições e respostas ARP de todas estações membros da VLAN possam ser capturadas, proceda como a seguir:

- selecione um filtro que capture apenas quadros do protocolo ARP e capture algumas dezenas de quadros;

- ao encerrar a captura analise os quadros capturados em busca de consultas ARP sem resposta. Ao encontrar consultas ARP sem resposta, analise quem enviou a consulta e que endereço IP deveria ser mapeado. Estas informações podem ajudar a descobrir qual o problema. Na Figura 11-1 apresentamos a decodificação de uma consulta ARP pelo Sniffer, da Network Associates. Nesta figura destacamos o endereço IP de quem solicitou a consulta. Mais abaixo, indicado pelo rótulo "Target protocolo address" está o endereço IP que deve ser mapeado para um endereço MAC. O endereço IP de quem solicitou a consulta ARP é indicado pelo rótulo "Sender's protocol address".

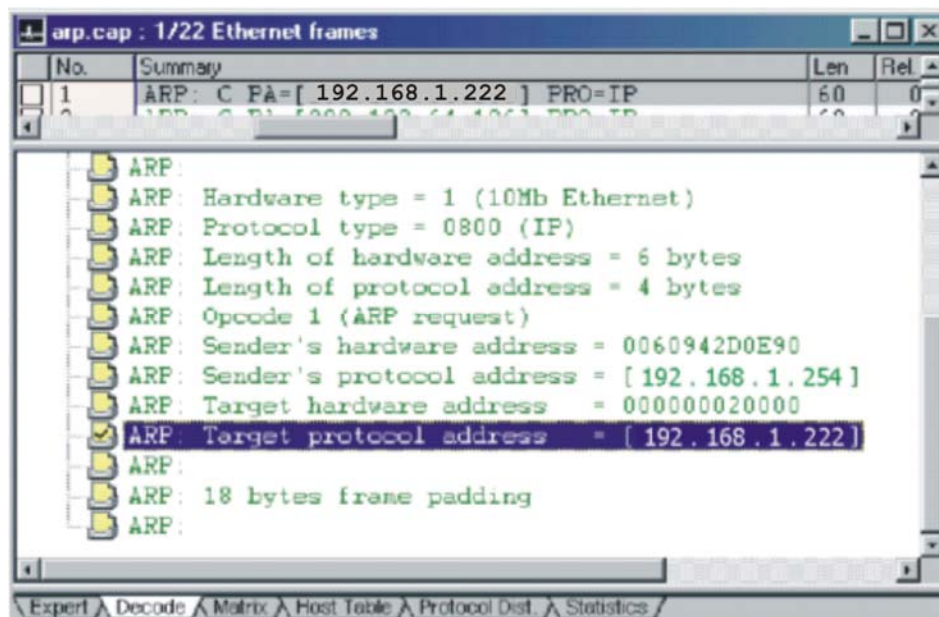



Figura 11-1: Decodificação de consulta ARP no Sniffer.

Se no domínio de difusão existir mais de um comutador, o procedimento será semelhante, mas a análise pode ser mais trabalhosa. Selecione no analisador um filtro que capture apenas quadros do protocolo ARP e inicie a captura. Capture algumas dezenas de quadros. Ao encerrar a captura analise o tráfego ARP capturado. Em muitas situações, quando você vir uma consulta ARP sem resposta não poderá concluir com certeza se esta é uma consulta ARP sem resposta, ou se a resposta simplesmente não foi capturada. A seguir encontram-se dicas de como analisar os dados capturados e como certificar-se de que a consulta realmente não foi respondida:

- estude as consultas ARP para as quais o analisador não capturou resposta alguma. Veja que máquina enviou a consulta e que endereço IP deveria ser mapeado. Com estas informações poderá ser possível concluir que: o endereço IP a ser mapeado não existe ou a máquina que fez a consulta não deveria estar participando do domínio de colisões em estudo;

- se após a análise descrita acima você ainda está com dúvidas sobre o que está ocorrendo, faça você mesmo esta consulta. Induza, a partir do seu analisador, uma consulta ARP que solicite o mesmo mapeamento da consulta ARP sem resposta;

- para tal, configure o seu analisador com endereço e máscara de rede apropriados. Deve ser possível que o analisador se comunique com as demais máquinas do domínio de difusão sob análise;

- envie mensagens ICMP Echo (`ping`) para a máquina cujo IP deve ser mapeado para endereço MAC. Por exemplo, suponha que você encontrou dentre os quadros capturados uma consulta ARP enviada pela máquina 192.168.1.204 solicitando o mapeamento ARP do endereço IP 192.168.1.222. Selecione o filtro de captura ARP no

analisador e inicie a captura. Então, a partir do próprio analisador de protocolos, direcione mensagens ICMP Echo para a máquina 192.168.1.222. Para que a comunicação entre o analisador e a máquina 192.168.1.222 seja possível será necessário descobrir o endereço MAC da máquina cujo IP é 192.168.1.222. A resposta a esta consulta será enviada ao próprio analisador. Encerre a captura e analise os dados capturados: a consulta foi respondida? Na realidade, se o `ping` foi respondido pela máquina 192.168.1.222 com sucesso, significa que a consulta ARP foi respondida. Mas, o oposto não é sempre verdade: se o `ping` não foi respondido com sucesso, não se pode concluir que a consulta ARP não foi respondida. Pode ser que a máquina remota esteja configurada para não responder `ping`. Por isso recomendamos que você capture os dados e os analise.

11.3 Obtendo tabela de rotas de roteadores

Neste procedimento serão apresentadas algumas maneiras de obtenção da tabela de rotas de roteadores e estações de trabalho.

11.3.1 Descrição e Dicas

Um roteador só é capaz de rotear adequadamente os datagramas que recebe se ele possuir uma tabela de rotas completa e sem erros. Em muitas situações você vai precisar analisar a tabela de rotas de seus equipamentos de interconexão em busca de problemas.

As tabelas de rotas de hospedeiros são tipicamente bastante simples. Basicamente existem duas entradas: uma que é utilizada quando o datagrama está destinado à mesma sub-rede do hospedeiro, e outra utilizada nos demais casos (a rota *default*).

As tabelas de rotas de roteadores, por outro lado, podem ser bem mais complexas. Para analisar corretamente a tabela de rotas de um roteador precisamos conhecer a topologia e o endereçamento da rede profundamente. Caso contrário não seremos capazes de decidir se a tabela está ou não correta.

Em geral, parte da tabela de rotas de um roteador é configurada estaticamente e parte dinamicamente através de protocolos como RIP e OSPF. Além de saber se as rotas estão corretas, devemos também verificar se cada rota foi aprendida como deveria ter sido, isto é, se ela foi inserida na tabela através de configuração manual ou através de protocolos de roteamento dinâmico.

Nas seções a seguir são dadas dicas de como obter tabelas de rotas de roteadores. Após obter a tabela de rotas você terá que analisá-la, para decidir se há ou não algum erro. Em geral, analisamos a tabela de rotas de um equipamento quando suspeitamos que ela está incorreta ou incompleta. É comum também que já tenhamos alguma suspeita de que erro está ocorrendo. Por exemplo, toda a rede do Departamento Financeiro está sem conectividade. A rede deste departamento é a 192.168.1.0/24. Então analisaremos nas tabelas

de rotas dos demais roteadores que rotas estão sendo seguidas quando a rede destino é a 192.168.1.0/24.

11.3.2 Usando uma estação de gerência SNMP

Nesta seção veremos que objetos SNMP trazem informações de tabelas de rotas.

A ipCidrRouteTable da IP *Forwarding Table* MIB [RFC2096] (a segunda atualização da tabela ipRouteTable da MIB-2) traz uma entrada para cada linha da tabela de rotas de um roteador. Em outras palavras, cada linha desta tabela representa uma entrada da tabela de rotas do equipamento sendo monitorado. Caminhar nesta tabela é o mesmo que caminhar na tabela de rotas do roteador.

O índice desta tabela é formado pelos objetos ipCidrRouteDest, ipCidrRouteMask, iipCidrRouteTos e ipCidrRouteNextHop. O objeto ipCidrRouteDest indica o endereço IP destino da rota (geralmente um endereço de rede). A variável colunar ipCidrRouteNextHop informa o endereço IP do roteador para o qual os datagramas destinados à rede ipCidrRouteDest devem ser entregues. ipCidrRouteMask informa a máscara de rede da rede destino (ipCidrRouteDest). Um AND lógico deve ser realizado entre esta máscara e o endereço destino contido no datagrama a ser roteado. O resultado desta operação é que será comparado com o endereço contido em ipCidrRouteDest. Você pode também obter a informação de como cada rota foi aprendida através do objeto ipCidrRouteProto.

11.3.3 Usando uma interface de linha de comando

Nesta seção veremos como obter a tabela de rotas em um roteador Cisco. Os comandos a serem executados dependem do fabricante e do modelo do roteador utilizado. Se os comandos apresentados aqui não valerem para o seu roteador, busque comandos correspondente nos manuais do seu equipamento.

Em roteadores Cisco com versão de IOS 10.0 ou superior use o seguinte comando:

```
roteador> show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
Gateway of last resort is 192.143.254.174 to network 0.0.0.0
C    192.168.64.0/24 is directly connected, FastEthernet1/0/0
O E1 192.17.251.0/24 [110/53] via 192.143.254.174, 02:28:54, ATM4/0/0.103
O E1 192.18.234.0/24 [110/53] via 192.143.254.174, 02:28:54, FastEthernet1/0/0
     192.211.38.0/30 is subnetted, 1 subnets
O E1 192.211.38.148 [110/52] via 192.143.254.174, 02:28:54, ATM4/0/0.103
```

```
O E1 192.137.174.0/24 [110/54] via 192.143.254.174, 02:29:24, ATM4/0/0.103
O E1 192.168.174.0/24 [110/54] via 192.143.254.174, 02:29:24, FastEthernet1/1/0
S    192.168.65.0/24 [1/0] via 192.168.64.131
S    192.168.66.0/24 [1/0] via 192.168.64.131
(…)
```

Quando nenhum parâmetro é passado, toda a tabela de rotas é apresentada, como exemplificado. Note que com este comando você pode ver cada entrada da tabela de rotas e como ela foi inserida – se estaticamente ou por algum protocolo de construção dinâmica de tabelas de rotas (RIP ou OSPF, por exemplo).

Se você quiser ver apenas a rota para determinada rede destino passe o endereço da rede destino como parâmetro:

```
roteador>show ip route 192.168.1.0
Routing entry for 192.168.1.0/24
  Known via "static", distance 1, metric 0
  Redistributing via ospf 1916
  Advertised by ospf 1916 metric 50 metric-type 1 subnets tag 145 route-
map I
  Routing Descriptor Blocks:
  * 192.168.64.131
      Route metric is 0, traffic share count is 1
```

Este resultado indica que a rota para a rede foi aprendida por configuração estática, que ela está sendo divulgada via o protocolo OSPF e que o próximo roteador que deve receber o datagrama com destinado à rede 192.168.1.0/24 é 192.168.64.131.

Você pode também observar apenas as rotas estáticas (parâmetro `static`), as redes diretamente conectadas (parâmetro `connected`) ou apenas as rotas aprendidas através de um determinado protocolo. Por exemplo, o comando seguinte apresenta apenas as rotas aprendidas através do protocolo OSPF:

```
roteador# show ip route ospf
```

Outros protocolos que podem ser passados como parâmetro são: `bgp`, `egp`, `eigrp`, `hello`, `igrp`, `isis` e `rip`.

Estes comandos são interessantes quando a tabela de rotas é grande e parte dela é configurada estaticamente e outra parte dinamicamente. Com eles você pode analisar a tabela por partes. Para tal você precisa saber perfeitamente como cada rota deve ser aprendida.

11.3.4 Usando netstat e route

Nesta seção apresentaremos como obter a tabela de rotas de máquinas com sistema operacional Linux ou Windows.

Em máquinas Linux os seguintes comandos apresentam a tabela de rotas configurada na máquina:

```
# netstat –nr
# route -n
```

Em máquinas com sistema operacional Windows execute o comando a seguir a partir de um *promp* de comandos:

```
C:\WINNT> route print
```

11.4 Verificando ocorrência de requisições DHCP sem resposta do servidor

Neste procedimento mostraremos como verificar se um cliente DHCP fica sem resposta do servidor DHCP após enviar mensagens DHCPDISCOVER ou DHCPREQUEST.

11.4.1 Descrição e Dicas

Leia mais sobre DHCP no apêndice 9

Em condições normais, após enviar uma mensagem a um servidor DHCP, o cliente recebe a resposta do servidor DHCP. Mensagens DHCPDISCOVER são respondidas pelo servidor com mensagens DHCPOFFER e mensagens DHCPREQUEST com uma mensagem DHCPACK ou DHCPNAK.

Se, por algum motivo, o cliente DHCP não receber resposta de um servidor, ele ficará tentando ainda se comunicar com este por algum tempo. Se ainda assim a comunicação não for possível, o cliente DHCP não poderá obter suas configurações de rede ou renová-las e, portanto, não poderá se comunicar através da rede. Alguns sistemas operacionais mostram ao usuário da máquina mensagens de erro quando o servidor DHCP não é alcançado.

Alguns problemas de rede podem interferir na comunicação entre servidor e cliente DHCP, de forma que o cliente envia mensagens de solicitação de endereço mas não recebe resposta alguma do servidor. Dentre estes problemas encontram-se: agente de repasse DHCP mal configurado e comutadores que não conseguem trocar informações sobre VLANs entre si. Estes problemas são descritos nas Seções 6.5 e 6.9 respectivamente.

11.4.2 Usando um analisador de protocolos

Veremos nesta seção como usar um analisador de protocolos para analisar a comunicação entre servidor e cliente DHCP.

Conecte o analisador de forma que ele possa capturar o tráfego DHCP entre o cliente e o servidor DHCP. Primeiramente, vamos conectar o analisador mais próximo do cliente. Escolha uma máquina cliente DHCP que não esteja conseguindo obter suas configurações de rede dinamicamente.

Selecione no analisador de protocolos um filtro que capture apenas mensagens do protocolo DHCP e inicie a captura. Durante a captura, force o cliente DHCP a enviar mensagens DHCPDISCOVER ou DHCPREQUEST ao

servidor. Isto pode ser feito em máquinas Windows com o comando `ipconfig /renew_all`. No Linux o comando a ser usado vai depender da implementação do cliente DHCP em uso. As implementações atualmente existentes são: `dhcpcd`, `pump` e `dhclient`. Para forçar um cliente dhcpcd a renovar configurações de rede com o servidor passe a opção `–n`:

```
# dhcpcd –n [interface]
```

Em clientes pump passe o parâmetro –R:

```
# pump –R [-i interface]
```

Uma outra forma de forçar o cliente DHCP a enviar estas mensagens é simplesmente reiniciá-lo.

Após forçar o envio de mensagens DHCPREQUEST pelo cliente, espere ainda alguns poucos minutos antes de encerrar a captura. Encerre a captura e analise os quadros capturados. O servidor DHCP respondeu à solicitação do cliente? Com o procedimento realizado até aqui já podemos concluir se o servidor DHCP está ou não respondendo as solicitações do cliente. Mas, outro teste pode ser realizado para descobrir informações adicionais.

Para descobrir onde a comunicação falha – se é a requisição DHCP que não chega no servidor ou a resposta deste que não chega no cliente – realize o mesmo procedimento com o analisador conectado mais próximo do servidor DHCP. Este teste adicional só precisa ser realizado quando cliente e servidor estiverem ligados a comutadores distintos ou quando um agente de repasse estiver sendo utilizado.

Selecione o filtro DHCP e inicie a captura. Durante a captura, force mais uma vez o cliente DHCP a enviar mensagens DHCPDISCOVER ou DHCPREQUEST. Após encerrar a captura verifique se as requisições do cliente chegaram até o servidor e se foram respondidas por ele.

11.4.3 Verificando logs do servidor DHCP

Podemos também obter informações sobre a comunicação entre cliente e servidor DHCP analisando os arquivos de *log* do servidor. Nem todos os servidores DHCP terão informações tão detalhadas. Apresentaremos nesta seção alguns eventos de *logs* do servidor DHCP do Windows 2000 e `dhcpd` que descrevem a comunicação entre cliente e servidor.

Force um cliente DHCP "com problemas" a enviar mensagens DHCPDISCOVER ou DHCPREQUEST ao servidor DHCP (dicas de como fazer isto são encontradas na Seção 11.4.2) e busque nos *logs* do servidor mensagens sobre esta comunicação. Se houver realmente problema na comunicação cliente/servidor DHCP nenhuma mensagem será encontrada no arquivo de *logs*.

WINDOWS 2000

Para que o servidor DHCP do Windows 2000 escreva arquivos de *logs* mais detalhados, habilite o *log* de auditoria da seguinte forma: na ferramenta de administração do DHCP (Iniciar > Programas > Ferramentas

Administrativas > DHCP) clique com o botão direito do mouse sobre o servidor DHCP e escolha o item Propriedades. Na tabela Geral clique em Habilitar Logging de Auditoria DHCP. Por *default*, o servidor criará um arquivo de *log* chamado DhcpSrvLog.xxx[61] no diretório winnt\system32\dhcp.

Os arquivos de *log* do servidor têm linhas com o seguinte formato:

ID, Data, Hora, Descrição, Endereço IP, Nome do hospedeiro, Endereço MAC

Na Tabela 11-1 cada um dos campos mencionados acima é descrito [ANALYZING-DHCP-LOG].

Campo	Descrição
ID	Um código de identificação de evento do servidor DHCP.
Data	A data na qual a mensagem de *log* foi escrita no arquivo de *log* do servidor DHCP.
Hora	A hora em que a entrada foi escrita no arquivo de *log* do servidor DHCP.
Descrição	Uma descrição deste evento do servidor DHCP.
Endereço IP	O endereço IP do cliente DHCP.
Nome do Hospedeiro	O nome do cliente DHCP.
Endereço MAC	O endereço MAC (Medium Access Control) do cliente DHCP.

Tabela 11-1: Descrição dos campos de uma entrada no arquivo de *logs* do servidor DHCP Windows 2000.

Na Tabela 11-2 são apresentadas algumas identificações de eventos do servidor DHCP que trazem informações sobre a comunicação cliente/servidor DHCP [ANALYZING-DHCP-LOG].

Identificação de evento	Descrição
10	Um novo endereço IP foi concedido a um cliente.
11	Uma concessão foi renovada pelo cliente.
12	Uma concessão foi liberada pelo cliente.
15	Uma concessão foi negada.

[61] Existe um *log* para cada dia. O arquivo de *log* da segunda-feira chama-se DhcpSrvLog.Mon, o da terça chama-se DhcpSrvLog.Tue e assim sucessivamente.

Tabela 11-2: Eventos que informam sobre a comunicação cliente/servidor DHCP.

DHCPD (LINUX)

Tipicamente, os *logs* do dhcpcd são escritos no arquivo /var/logs/messages ou /var/adm/messages, dependendo do seu sistema. Veja a seguir um exemplo da gravação de uma conversa entre servidor e cliente no arquivo de *logs*:

Apr 12 10:15:37 mingau dhcpd: **DHCPDISCOVER** from 00:10:b5:61:b2:65 via eth0
Apr 12 10:15:38 mingau dhcpd: **DHCPOFFER** on 192.168.4.1 to 00:10:b5:61:b2:65 (Computador) via eth0
Apr 12 10:15:38 mingau dhcpd: **DHCPREQUEST** for 192.168.4.1 (200.129.64.153) from 00:10:b5:61:b2:65 (Computador) via eth0
Apr 12 10:15:38 mingau dhcpd: **DHCPACK** on 192.168.4.1 to 00:10:b5:61:b2:65 (Computador) via eth0

11.5 Verificando se log do servidor DHCP indica falta de endereços IP

Neste procedimento daremos algumas dicas de como verificar nos logs do serviço DHCP implementações ISC e Windows 2000 se está faltando endereços para os clientes DHCP.

11.5.1 Descrição e dicas

No arquivo de *logs* dos servidores DHCP podemos encontrar mensagens que nos ajudam a descobrir problemas e entender melhor seu comportamento. Muitas mensagens interessantes e importantes são escritas nos arquivos de *logs* do DHCP. Mas, neste procedimento, falaremos apenas das mensagens escritas quando o servidor quer nos avisar que não possui mais endereços disponíveis para oferecer aos clientes. É importante que você esteja sempre atento aos arquivos de *logs* do servidor DHCP e que saiba interpretá-los adequadamente.

11.5.2 Verificando logs do servidor

Nesta seção veremos onde se localizam os logs do serviço DHCP ISC e Windows 2000. Veremos também que mensagens estes logs contêm quando o servidor DHCP não mais tiver endereços a oferecer aos seus clientes.

DHCP ISC

O servidor DHCP oferecido pela ISC (*Internet Software Consortium*) enviará mensagens para o arquivo de log através do syslog. Por *default*, as mensagens de *log* do DHCP serão encontradas juntamente com mensagens de *logs* de todos os outros *daemons* que também usam o syslog. Tipicamente estas mensagens são encontradas em /var/log/messages ou /var/adm/messages, dependendo do seu sistema.

Quando faltam endereços IP as mensagem de erro "no free leases" é encontrada no arquivo de *logs* do servidor DHCP ISC. Se você encontrar neste arquivo uma mensagem de *log* que você não entende, aí vai uma dica: pesquise no arquivo dhcp.c do servidor ISC as mensagens de *log*. Procure as chamadas das funções log_error ou log_info. Leia os comentários escritos próximos a estas chamadas. Em geral eles descrevem o que causa o envio da mensagem de *log*.

DHCP WINDOWS 2000

No Windows 2000, informações de inicialização e término do serviço DHCP são visualizadas através do Event Viewer. Quando queremos obter informações de *logs* mais detalhadas temos que habilitar o sistema de *logging*. Isto é feito conforme explicado na Seção 11.4.3.

Quando o servidor DHCP não tiver endereços disponíveis para oferecer a um cliente DHCP ele informará o erro no arquivo de *logs*. No Windows 2000 o evento identificado pelo número 14 indica que uma requisição não foi satisfeita porque não existiam mais endereços IP disponíveis no escopo. Conheça outras identificações de eventos do servidor DHCP Windows em [ANALYZING-DHCP-LOG, WIN-TIP412].

11.6 Verificando ocorrência de mensagens DHCPNAK na rede

Neste procedimento mostraremos como verificar se servidores DHCP estão constantemente enviando mensagens DHCPNAK para os clientes DHCP.

11.6.1 Descrição e Dicas

Mensagens DHCPNAK são enviadas pelo servidor DHCP a um cliente DHCP nas seguintes situações [RFC2131]:

- o cliente DHCP solicita o aluguel de um endereço IP que não faz parte da faixa de endereços IP configurada no servidor DHCP. Isto é comum quando um cliente é transferido de uma rede para outra. O cliente ainda se lembra do último endereço alocado a ele, mas este endereço faz parte de outra rede;

- o cliente DHCP solicita renovar o aluguel de seu endereço, mas o tempo de concessão do mesmo já expirou.

Quando mensagens DHCPNAK são constantemente enviadas pelo servidor DHCP mesmo que nenhuma máquina tenha sido transferida de uma rede para outra, desconfie que o número de máquinas na rede está bem maior que o número de endereços IP que podem ser concedidos pelo servidor. Desta forma, o servidor não está conseguindo manter um cliente DHCP com o mesmo endereço IP por muito tempo.

Mesmo quando usamos DHCP podemos ter um certo conhecimento sobre qual IP está alocado às máquinas da rede. O servidor DHCP esforça-se para sempre permitir que uma máquina permaneça com o mesmo endereço IP que ela recebeu na primeira alocação dinâmica pelo maior tempo possível. Mesmo que o tempo de concessão de um endereço tenha expirado, o servidor DHCP não concederá este endereço a um outro cliente, exceto se não houver outro endereço IP disponível.

11.6.2 Usando um analisador de protocolos

Veremos nesta seção como verificar com o auxílio de um analisador de protocolos se mensagens DHCPNAK estão sendo constantemente enviadas do servidor DHCP para clientes DHCP.

Conecte o analisador de protocolos de forma que ele possa enxergar todo o tráfego do servidor DHCP. Se ainda não existir, crie um filtro que selecione apenas quadros que carregam dados do protocolo DHCP para captura. Selecione o filtro DHCP e inicie a captura. É interessante que você passe algum tempo capturando quadros, pelo menos um tempo inicial de 1 hora. É também recomendado que este procedimento seja realizado em um horário de pico, em que existam vários clientes DHCP ativos.

Após encerrar a captura verifique a existência de mensagens DHCPNAK dentre os quadros capturados. Se nenhuma mensagem DHCPNAK foi encontrada dentre os quadros capturados, não podemos concluir com certeza que estas mensagens não estejam sendo transmitidas aos clientes em algum momento. Para ser mais conclusivo, você pode iniciar uma nova captura que dure mais algum tempo. Se quiser faça várias capturas e verifique se dentre os dados capturados existem mensagens DHCPNAK.

11.6.3 Verificando logs do servidor DHCP

O envio de uma mensagem DHCPNAK deve ser gravada no arquivo de *logs* do servidor DHCP. Nesta seção veremos um exemplo da mensagem de *log* gravada pela implementação `dhcpd` da ISC ao enviar uma mensagem DHCPNAK. Esta verificação é mais conclusiva que a anterior, realizada com o analisador de protocolos, sendo, portanto, mais recomendada.

Veja abaixo a mensagem gravada pelo servidor dhcpd ao enviar DHCPNAK:

```
Apr 12 11:00:13 servidor dhcpd: DHCPNAK on 192.168.4.1 to 00:04:ac:ee:c7:db via eth0
```

Provavelmente, o IP 192.168.4.1 foi liberado pelo cliente (que recebeu a mensagem DHCPNAK) há algum tempo, mas agora ele pretende renovar a concessão. No entanto, enquanto este cliente estava inativo, o IP em questão já foi concedido a outro cliente DHCP.

11.7 Analisando requisições de clientes DHCP externos

Neste procedimento, estudaremos as requisições de clientes DHCP que estão em um outro domínio de difusão e usam um agente de repasse DHCP para se comunicar com um servidor DHCP.

11.7.1 Descrição e Dicas

Um agente de repasse é um hospedeiro ou roteador que repassa mensagens DHCP entre clientes e servidores que não participam de um mesmo domínio de

difusão. Usando agentes de repasse eliminamos a necessidade de se ter um servidor DHCP em cada domínio de difusão.

Quando agentes de repasse são utilizados, o servidor DHCP passa a receber requisições deste agente. Quando o agente de repasse está mal configurado ou quando existe um filtro IP barrando o tráfego DHCP entre o agente de repasse e o servidor DHCP, as requisições de clientes que usam o agente de repasse não chegarão ao servidor DHCP.

Na próxima seção veremos como usar um analisador de protocolos para checar o tráfego DHCP entre o agente de repasse e o servidor DHCP.

11.7.2 Usando um analisador de protocolos

Mostraremos nesta seção como analisar o tráfego DHCP entre um servidor e um agente de repasse DHCP com o auxílio de um analisador de protocolos.

O primeiro passo é conectar o analisador de forma que ele possa enxergar as mensagens DHCP enviadas do agente de repasse para o servidor DHCP. Selecione um filtro que capture apenas mensagens DHCP e inicie a captura. Dicas de como conectar o analisador e como criar este filtro no Sniffer, da Network Associates, podem ser encontradas no **UTILIZANDO UM ANALISADOR DE PROTOCOLOS**.

Durante a captura, force a comunicação entre clientes DHCP que usam o agente de repasse e o servidor DHCP. Isto pode ser feito em clientes DHCP Windows usando o comando `ipconfig /renew_all`. Em máquinas Linux o comando a ser utilizado depende da implementação do cliente DHCP instalada. Para forçar um cliente dhcpcd a renovar configurações de rede com o servidor passe a opção `–n`:

```
# dhcpcd –n [interface]
```

Em clientes pump passe o parâmetro –R:

```
# pump –R [-i interface]
```

Outra forma de forçar o cliente DHCP a comunicar-se com o servidor é simplesmente reiniciar a máquina cliente. Assim, certamente capturaremos quadros com mensagens DHCP enviadas pelo agente de repasse.

Após encerrar a captura analise os quadros capturados. Verifique especialmente para que endereço as mensagens DHCP estão sendo enviadas. O endereço IP destino destas mensagens é mesmo o endereço IP do servidor DHCP que deve lidar com esta requisição? Se nenhuma mensagem DHCP foi capturada você provavelmente tem um problema com o seu agente de repasse. Você pode conectar um analisador de protocolos próximo ao cliente DHCP para certificar-se de que ele realmente está enviando requisições DHCP. Se você verificou que o agente de repasse está enviando corretamente as requisições DHCP para o servidor DHCP, mas os clientes DHCP que usam o agente continuam sem poder obter suas configurações de rede, continue o procedimento como descrito a seguir:

- conecte o analisador de protocolos de forma que ele possa capturar todo o tráfego do servidor DHCP;
- selecione o filtro de captura DHCP e inicie a captura;
- mais uma vez, force clientes DHCP externos a realizarem requisições DHCP;
- ao encerrar a captura analise os quadros capturados. Dentre eles você encontra quadros transmitidos pelo agente de repasse?

11.8 Verificando existência de mensagens ICMP de redirecionamento na rede

Neste procedimento veremos como verificar se os roteadores da rede estão enviando muitas mensagens ICMP de redirecionamento. Além disso, descreveremos como um analisador de protocolos pode nos ajudar a obter mais dados sobre as mensagens ICMP de redirecionamento encontradas na rede.

11.8.1 Descrição e dicas

Mensagens ICMP de redirecionamento (tipo 5, código 0-3) são enviadas por roteadores na seguinte situação [RFC 792]:

- ao receber um datagrama IP, um roteador consulta sua tabela de rotas em busca do próximo roteador para o qual o datagrama deve ser enviado. Se o roteador perceber que o próximo roteador e a máquina que originou o datagrama fazem parte da mesma rede, o roteador envia uma mensagem ICMP de redirecionamento para a máquina origem do datagrama. A origem, por sua vez, incluirá em sua tabela de rotas a nova rota, temporariamente.

Em resumo, uma mensagem ICMP de redirecionamento é enviada para informar a um hospedeiro que ele deveria usar uma outra rota (melhor) ao tentar se comunicar com certos destinos.

Apenas roteadores podem enviar mensagens ICMP de redirecionamento. Quando um hospedeiro recebe uma mensagem ICMP de redirecionamento ele deve agir da seguinte maneira [RFC1122]:

- acrescentar uma nova rota na tabela de rotas apropriadamente;
- descartar a mensagem de redirecionamento se ela indicar um roteador que não possui o mesmo prefixo de rede da interface pela qual a mensagem ICMP de redirecionamento chegou. Por exemplo, se um hospedeiro recebe pela sua interface cujo endereço é 192.168.1.24 uma mensagem de redirecionamento, ele pode descartar esta mensagem se ela indicar que datagramas destinados a uma certa máquina devem ser entregues ao roteador 192.168.2.254;

- descartar a mensagem de redirecionamento se ela não tiver sido enviada pelo primeiro roteador ao qual o datagrama que causou sua transmissão foi entregue.

Segundo [RFC1812] um roteador com protocolos de roteamento dinâmico ativos deve descartar mensagens ICMP de redirecionamento destinadas a ele.

Em geral, a existência de tráfego de mensagens ICMP de redirecionamento na rede indica tabelas de rotas incorretas ou incompletas em hospedeiros. Felizmente, estes erros em tabelas de rotas não causarão a falta de conectividade na rede. Ao enviar uma mensagem de redirecionamento um roteador apenas está tentando ensinar à origem de um datagrama um caminho mais curto para entregá-lo ao destino.

11.8.2 Usando uma estação de gerência SNMP

Apresentamos nesta seção objetos SNMP que informam a quantidade de mensagens ICMP de redirecionamento recebida e enviada por um equipamento. Estes objetos são definidos no grupo ICMP da MIB-2 [RFC1213]:

- o objeto icmpInRedirects é um contador do grupo conta a quantidade de mensagens ICMP de redirecionamento recebida por um equipamento. Por exemplo, sempre que uma máquina A receber uma mensagem ICMP de redirecionamento, o contador icmpInRedirects será incrementado. Portanto, com o auxílio deste contador, você pode descobrir se um hospedeiro está recebendo com freqüência mensagens ICMP de redirecionamento;

- o objeto icmpOutRedirects conta a quantidade de mensagens ICMP de redirecionamento enviada por um equipamento. Apenas roteadores enviam mensagens deste tipo, portanto só faz sentido monitorar estes objetos em roteadores.

Como estes objetos são contadores, devemos identificar seu incremento em um determinado intervalo de tempo. Considere que o intervalo de coleta de dados ICMP é T. Em duas coletas de dados consecutivas os valores do contador ipInRedirects obtidos de um equipamento foram $ipInRedirects_0$ e $ipInRedirects_{0+T}$. Então, durante o tempo T, o equipamento em questão recebeu $ipInRedirects_{0+T}$ - $ipInRedirects_0$ mensagens ICMP de redirecionamento.

11.8.3 Usando uma interface de linha de comando

Nesta seção apresentaremos como verificar se roteadores Cisco estão enviando ou recebendo muitas mensagens ICMP de redirecionamento. Se você possui roteadores produzidos por outro fabricante, procure nos manuais do seu equipamento comandos que possam lhe informar dados sobre mensagens ICMP.

Em roteadores Cisco com versão de IOS superior a 10.0, execute o comando a seguir para visualizar estatísticas do tráfego IP:

```
show ip traffic
```

Veja um exemplo do resultado deste comando onde destacamos contadores de mensagens ICMP de redirecionamento recebidas e enviadas:

```
roteador> show ip traffic
(…)
ICMP statistics:
  Rcvd: 0 format errors, 19 checksum errors, 1 redirects, 31 unreachable
        209227 echo, 11 echo reply, 0 mask requests, 0 mask replies, 0
quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        18 irdp solicitations, 0 irdp advertisements
  Sent: 961458 redirects, 7934 unreachable, 10 echo, 209227 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 106591 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
(…)
```

Se o roteador estiver enviando muitas mensagens de redirecionamento, o ideal é descobrir para quem estas mensagens estão sendo enviadas e qual o endereço destino dos datagramas que causam o envio destas mensagens. Mas, estas informações só podem ser descobertas com um auxílio de um analisador de protocolos, como você verá na próxima seção.

11.8.4 Usando um analisador de protocolos

Nesta seção veremos como usar um analisador de protocolos para analisar o tráfego ICMP de redirecionamento em uma rede.

Conecte o analisador de protocolos de forma que ele possa capturar as mensagens ICMP que você deseja. Neste ponto, você deve estar tentando analisar as mensagens ICMP de redirecionamento enviadas por um roteador, recebidas por um hospedeiro ou ainda as mensagens ICMP de redirecionamento destinadas ou originadas em redes externas.

De forma geral, você estará tentando capturar mensagens ICMP que trafegam entre dois equipamentos. Conecte o analisador de protocolos de forma que ele capture os dados desejados, seguindo as dicas oferecidas no **UTILIZANDO UM ANALISADOR DE PROTOCOLOS**.

Em seu analisador de protocolos crie/selecione um filtro que capture apenas quadros que contenham mensagens ICMP. No analisador de protocolos Sniffer, da Network Associates, este filtro pode ser criado como descrito na Seção 9.1.2 (página 222). Você pode ainda criar um filtro mais detalhado que capture apenas mensagens ICMP de redirecionamento.

Selecione o filtro desejado e capture dados por alguns minutos. Após encerrar a captura decodifique os quadros capturados. Verifique para quem as mensagens

estão sendo enviadas, isto é, olhe o endereço IP destino dos datagramas capturados. Além disso, veja qual a rota envolvida no erro.

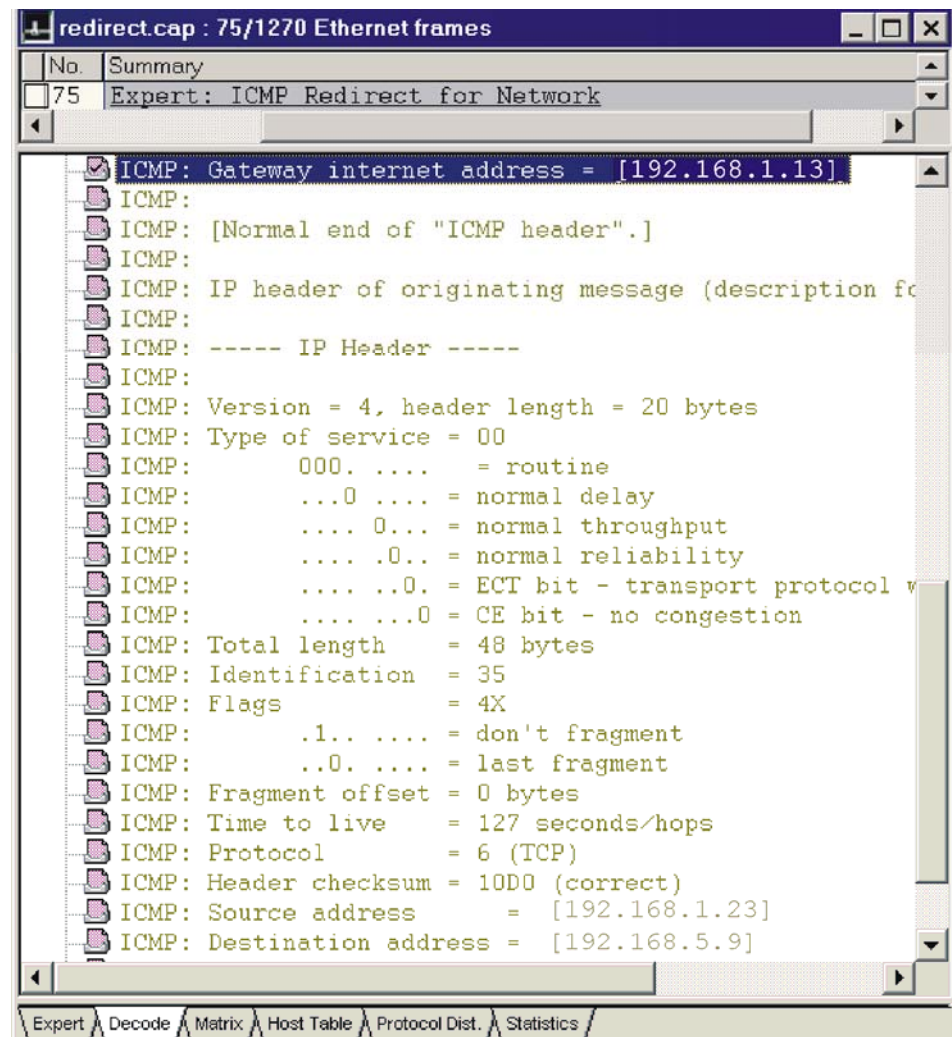



Figura 11-2: Decodificação de uma mensagem ICMP de redirecionamento no Sniffer.

Na Figura 11-2 apresentamos um quadro que carrega uma mensagem ICMP de redirecionamento. Note que este quadro carrega o cabeçalho IP do datagrama original que causou o envio da mensagem de redirecionamento. Com os dados contidos na mensagem ICMP podemos portanto descobrir: 1) o endereço do roteador que deve ser usado como melhor rota; 2) a máquina que enviou o datagrama que causou o envio da mensagem de redirecionamento e 3) o endereço destino que pode ser alcançado a partir de um rota melhor. Todas estas informações podem ser vistas no quadro decodificado na Figura 11-2.

Nesta figura destacamos o endereço (192.168.1.13) do próximo roteador que deve ser usado pela máquina 192.168.1.23 ao transmitir dados para o destino 192.168.5.9.

11.9 Analisando tráfego de mensagens ICMP Time Exceeded

Neste procedimento veremos como verificar se os roteadores da rede estão enviando muitas mensagens ICMP de TTL excedido em trânsito. Além disso, descreveremos como um analisador de protocolos pode nos ajudar a estudar melhor as mensagens ICMP de TTL excedido em trânsito que trafegam na rede.

11.9.1 Descrição e dicas

Existem dois códigos para mensagens de controle ICMP *Time Exceeded*: tempo de vida excedido em trânsito (código 0) e tempo de remontagem de fragmentos excedido (código 1).

Quando um roteador observa que o valor do TTL de um datagrama sendo processado vai cair para zero, o datagrama é descartado, e uma mensagem de tempo de vida excedido é enviado para a máquina que originou o datagrama (endereço fonte do datagrama).

Se um hospedeiro não puder remontar um datagrama porque faltam fragmentos do mesmo, ele descarta o datagrama e envia uma mensagem de tempo excedido durante remontagem para a origem do datagrama.

Mensagens ICMP *Time Exceeded*, idealmente, não deveriam trafegar na rede. Se uma mensagem ICMP de tempo excedido é encontrada esporadicamente, não há problema. No entanto, se estes tipos de mensagens estão sempre presentes em sua rede uma investigação mais detalhada faz-se necessária.

Neste procedimento estamos preocupados em lhe mostrar como verificar se seus roteadores estão enviando muitas mensagens ICMP de TTL excedido (código 0).

11.9.2 Usando uma estação de gerência SNMP

Nesta seção veremos como uma estação de gerência SNMP pode auxiliar na detecção de mensagens ICMP de TTL excedido na rede.

O contador icmpOutTimeExcds do grupo ICMP da MIB-2 [RFC1213] é incrementado cada vez que uma mensagem ICMP de tempo excedido é transmitida.

Em geral, mensagens ICMP de TTL excedido só são enviadas por roteadores e apenas hospedeiros enviam mensagens ICMP de tempo de remontagem excedido. Portanto, a variável icmpOutTimeExcds, quando obtida de roteadores, informa a quantidade de mensagens ICMP de TTL excedido enviadas por eles.

Lembre-se que esta variável é um contador, e que o seu valor absoluto nada significa. O importante é saber o valor do incremento desta variável no tempo. Por exemplo, colete dados SNMP de 5 em 5 minutos. Em uma determinada coleta, você encontrou que $\text{icmpOutTimeExcds}_0$ continha o valor 8.000.000.

Este número nada significa. Você só pode concluir se há ou não problemas na rede quando tiver em mãos o valor da variável icmpOutTimeExcds na próxima coleta. Suponha que na próxima coleta o valor da variável é 8.000.500. Isto significa que em 5 minutos, o roteador enviou 500 mensagens ICMP de TTL excedido. Foi uma média de 100 mensagens por minuto, ou quase 2 mensagens por segundo. Este é um número bastante alto. É provável que existam problemas de roteamento em sua rede, ou ainda que ela esteja sendo atacada.

11.9.3 Usando uma interface de linha de comando

Apresentaremos nesta seção como obter a quantidade de mensagens ICMP de TTL excedido enviada por roteadores Cisco. Se você possui roteadores produzidos por outro fabricante procure nos manuais dos seus equipamentos os comandos correspondentes aos que serão apresentados aqui.

Em um roteador Cisco com IOS versão 10.0 ou superior, execute o comando:

```
roteador> show ip traffic
IP statistics:
(…)
ICMP statistics:
  Rcvd: 0 format errors, 1 checksum errors, 0 redirects, 5 unreachable
        27150 echo, 1 echo reply, 0 mask requests, 0 mask replies, 0
quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 146052 redirects, 36 unreachable, 0 echo, 27150 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 7863 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
(…)
```

Este comando oferece estatísticas de vários protocolos da pilha TCP/IP, dentre eles, o ICMP. O número de mensagens ICMP de tempo excedido transmitido pelo roteador está em negrito no exemplo. Este número é um contador, , portanto, será necessário recuperar o seu valor em dois momentos distintos e ver quantas mensagens ICMP de tempo excedido foram realmente enviadas neste intervalo de tempo.

11.9.4 Usando um analisador de protocolos

Nesta seção veremos como usar um analisador de protocolos para verificar se mensagens ICMP de TTL excedido estão sendo constantemente enviada por roteadores da rede e veremos como obter dados sobre estas mensagens.

Com um analisador de protocolos você não poderá observar a quantidade total de mensagens ICMP de TTL excedido por todas as interfaces do roteador de uma só vez. Pode observar apenas as mensagens enviadas por uma interface de cada vez. Em compensação, com o analisador podemos ver o cabeçalho do datagrama que gerou a mensagem (que teve o TTL zerado). De onde ele veio e para onde ele deveria ter ido. Estas informações nos ajudam a determinar ou entender melhor o problema que está ocorrendo.

Conecte o analisador de protocolos de forma que ele capture os dados transmitidos e recebidos pela interface do roteador que você deseja testar. Após conectar o analisador, capture mensagens ICMP. Dicas de como conectar o analisador e criar filtros de captura (no Sniffer, da Network Associates) são encontradas no **UTILIZANDO UM ANALISADOR DE PROTOCOLOS**.

Se a taxa de captura estiver muito alta, capture algumas centenas de quadros. Se raríssimos quadros estão sendo capturados espere alguns minutos (10 minutos, por exemplo), antes de encerrar a captura.

Finalmente, ao encerrar a captura, analise os quadros capturados. A mensagem ICMP de TTL excedido em trânsito traz consigo o cabeçalho IP do datagrama cujo TTL chegou a zero. Desta forma, podemos saber quem enviou o datagrama e para que destino. A Figura 11-3 mostra a decodificação de uma mensagem ICMP de TTL excedido em trânsito. Em destaque está o IP fonte (192.168.14.130) do datagrama cujo TTL excedeu e em seguida o IP destino. Ao analisar esta mensagem descobrimos que existe um problema de comunicação entre 192.168.14.130 e 192.168.2.132.

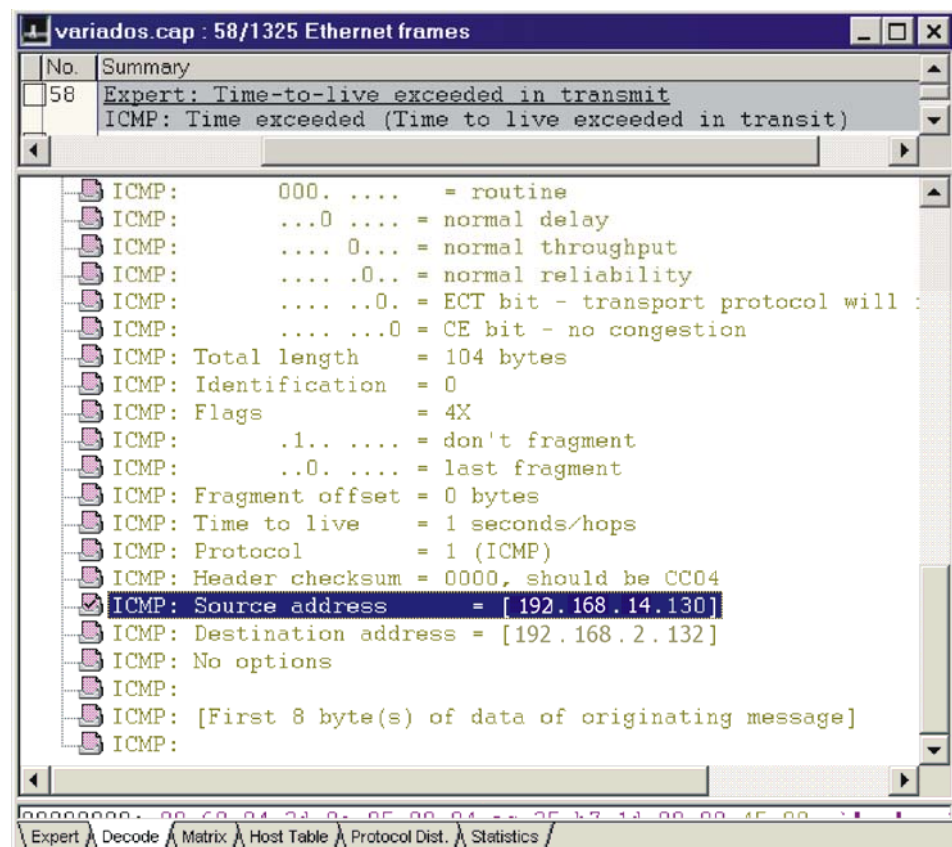



Figura 11-3: Decodificação de uma mensagem ICMP de TTL excedido em trânsito.

11.10 Analisando tráfego de mensagens ICMP de destino inalcançável

Neste procedimento descreveremos em que circunstâncias um equipamento envia mensagens ICMP de destino inalcançável para outro equipamento e como analisar o tráfego deste tipo de mensagens em uma rede.

11.10.1 Descrição e Dicas

Existem vários tipos de mensagens ICMP de destino inalcançável. Algumas delas são enviadas por roteadores, outras por hospedeiros. Antes de descartar qualquer datagrama, o roteador/hospedeiro envia uma mensagem ICMP de destino inalcançável para a origem do mesmo reportando que o destino é (ou está) inalcançável.

Mensagens ICMP de destino inalcançável têm sempre o código 3. Existem vários tipos de mensagens ICMP de destino inalcançável, mas neste procedimentos trataremos apenas dos apresentados na Tabela 11-3.

Código	Descrição
0	Rede inalcançável. Quando um roteador recebe um datagrama mas não possui uma rota que sirva para levá-lo até o seu destino, o roteador envia para a origem do datagrama uma mensagem ICMP de rede inalcançável. Esta mensagem é geralmente enviada por roteadores com tabelas de rotas incompletas ou quando o endereço destino do datagrama não existe.
1	Hospedeiro inalcançável. Quando um roteador tenta fazer uma entrega direta ao destino final, mas este não está alcançável. A máquina está desligada ou fora de serviço.
3	Porta inalcançável. Quando o destino final recebe um datagrama mas não existem processos para tratá-lo na porta especificada como porta destino.

Tabela 11-3 Alguns códigos de mensagens ICMP de destino inalcançável.

Mensagens ICMP de destino inalcançável são consideradas mensagens de erro. Se poucas mensagens ICMP de destino inalcançável são esporadicamente encontradas na rede não se preocupe. Mas se elas estão sempre presentes e em grande quantidade, é bom analisá-las melhor, pois elas podem lhe dar dicas sobre o que está ocorrendo de errado na rede.

11.10.2 Usando uma estação de gerência SNMP

Nesta seção veremos como uma estação de gerência SNMP pode oferecer informações sobre o tráfego de mensagens ICMP de destino inalcançável.

As seguintes variáveis de gerência da MIB-2 [RFC1213] podem ser úteis:

- IcmpInDestUnreachs → conta a quantidade de mensagens ICMP de destino inalcançável recebidas pelo equipamento;

- IcmpOutDestUnreachs → conta a quantidade de mensagens ICMP de destino inalcançável transmitidas pelo equipamento;

As variáveis apresentadas são do tipo contador, por isso precisamos descobrir o seu incremento ao longo de um determinado intervalo de tempo. Para saber, por exemplo, se um roteador está enviando muitas mensagens ICMP de destino inalcançável precisamos obter o valor de IcmpOutDestUnreachs, esperar um certo tempo e depois obter o valor desta variável novamente. A diferença de valores entre a primeira e a segunda coletas informa se o roteador está ou não transmitindo muitas mensagens de destino inalcançável.

Não é comum que roteadores recebam mensagens ICMP de destino inalcançável. Se um roteador recebe uma mensagem deste tipo significa que ele está originando os datagramas que causam o envio de mensagens de destino inalcançável. Excetuando-se dados de controle de roteamento transmitidos por protocolos como RIP e OSPF, tráfego SNMP, mensagens de *logs*[62] e sessões de `telnet`, um roteador não é a origem de datagramas, é apenas um repassador destes.

Se um roteador está enviando muitas mensagens ICMP de destino inalcançável, algum problema está ocorrendo na rede, e merece uma investigação. Infelizmente, com uma estação de gerência SNMP não podemos saber que tipo de mensagem ICMP de destino inalcançável está sendo recebida/transmitida pelos equipamentos da rede. Não podemos também saber que endereço ou porta destino gerou a mensagem de destino inalcançável. Na Seção **USANDO UM ANALISADOR DE PROTOCOLOS** você verá como realizar esta investigação usando um analisador de protocolos.

11.10.3 Usando uma interface de linha de comando

Apresentaremos nesta seção como obter a quantidade de mensagens ICMP de destino inalcançável enviada/recebida por roteadores Cisco. Se você possui roteadores produzidos por outro fabricante procure nos manuais dos seus equipamentos os comandos correspondentes aos que serão apresentados aqui.

Em um roteador Cisco com IOS versão 10.0 ou superior, execute o comando:

```
roteador> show ip traffic
IP statistics:
(…)
ICMP statistics:
  Rcvd: 0 format errors, 1 checksum errors, 0 redirects, 5 unreachable
        27150 echo, 1 echo reply, 0 mask requests, 0 mask replies, 0
quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
```

[62] O roteador pode estar configurado para escrever *logs* em um hospedeiro.

```
  Sent: 146052 redirects, 36034 unreachable, 0 echo, 27150 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 7863 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
(…)
```

As quantidades de mensagens ICMP de destino inalcançável transmitidas e recebidas pelo roteador estão em negrito. Estes valores são contadores, portanto, será necessário recuperá-los em dois momentos distintos e ver quantas mensagens ICMP de destino inalcançável foram realmente enviadas neste intervalo de tempo.

Utilizando uma interface de linha de comando não será também possível obter informações sobre o tipo de mensagem de destino inalcançável transmitida/recebida pelo roteador.

11.10.4 Usando um analisador de protocolos

Quando você desejar realizar uma investigação mais profunda sobre o tráfego de mensagens ICMP de destino inalcançável use um analisador de protocolos. Nesta seção veremos como proceder.

Você descobriu que um roteador está enviando muitas mensagens ICMP de destino inalcançável e resolveu analisar melhor estas mensagens usando um analisador de protocolos. Para descobrir através de qual interface do roteador as mensagens ICMP estão sendo enviadas será necessário analisar o tráfego em cada uma delas. Conecte o analisador de protocolos adequadamente, como descrito no **UTILIZANDO UM ANALISADOR DE PROTOCOLOS**.

Se você desconfia que as mensagens ICMP estão sendo enviadas para máquinas não locais, você pode conectar seu analisador em um enlace por onde passe todo o tráfego de saída da rede interna. Conectar o analisador de protocolos de forma que ele enxergue todo o tráfego de saída da rede interna é interessante porque você pode ver todas as mensagens ICMP enviadas por todos os roteadores da rede interna para máquinas externas.

Crie/selecione um filtro que capture apenas mensagens ICMP. Dicas para a criação deste filtro no Sniffer, da Network Associates, podem ser encontradas na Seção **9.1.2 CRIANDO E SELECIONANDO FILTROS DE CAPTURA**.

Capture mensagens ICMP durante alguns minutos. Em seguida analise as mensagens ICMP de destino inalcançável capturadas. Em primeiro lugar, olhe o tipo das mensagens capturadas. Como dissemos na Seção **DESCRIÇÃO E DICAS**, existem vários tipos de mensagens ICMP de destino inalcançável, cada um deles reportando um certo tipo de erro.

Observe o endereço IP origem e destino das mensagens ICMP de destino inalcançável capturadas. Assim, você saberá que roteador está enviando estas mensagens e que máquina enviou um datagrama para um destino/porta inalcançável. Na Figura 11-4 destacamos o endereço IP (192.168.2.1) do roteador que enviou a mensagem ICMP de destino inalcançável.

Uma outra análise interessante pode ser realizada quando se tratam de mensagens ICMP de rede ou hospedeiro inalcançáveis. Toda mensagem ICMP carrega o cabeçalho IP do datagrama que gerou a mensagem. Isto significa que podemos saber qual o destino que está inalcançável. Na Figura 11-5 destacamos o endereço IP destino (192.168.1.6) do datagrama original que causou o envio da mensagem ICMP de destino inalcançável, isto é, o endereço IP da máquina que está inalcançável.

Quando se tratam de mensagens ICMP de portas inalcançáveis é interessante saber também que porta está envolvida. Infelizmente, na mensagem ICMP apenas o cabeçalho do datagrama que gerou a mensagem é anexado. Isto significa que ao analisar uma mensagem ICMP de porta inalcançável podemos saber que máquina gerou a mensagem, mas não podemos saber que porta foi acessada. Para descobrir que porta está envolvida, comece a capturar os dados originados nas máquinas para as quais as mensagens ICMP de portas inalcançáveis foram destinadas.

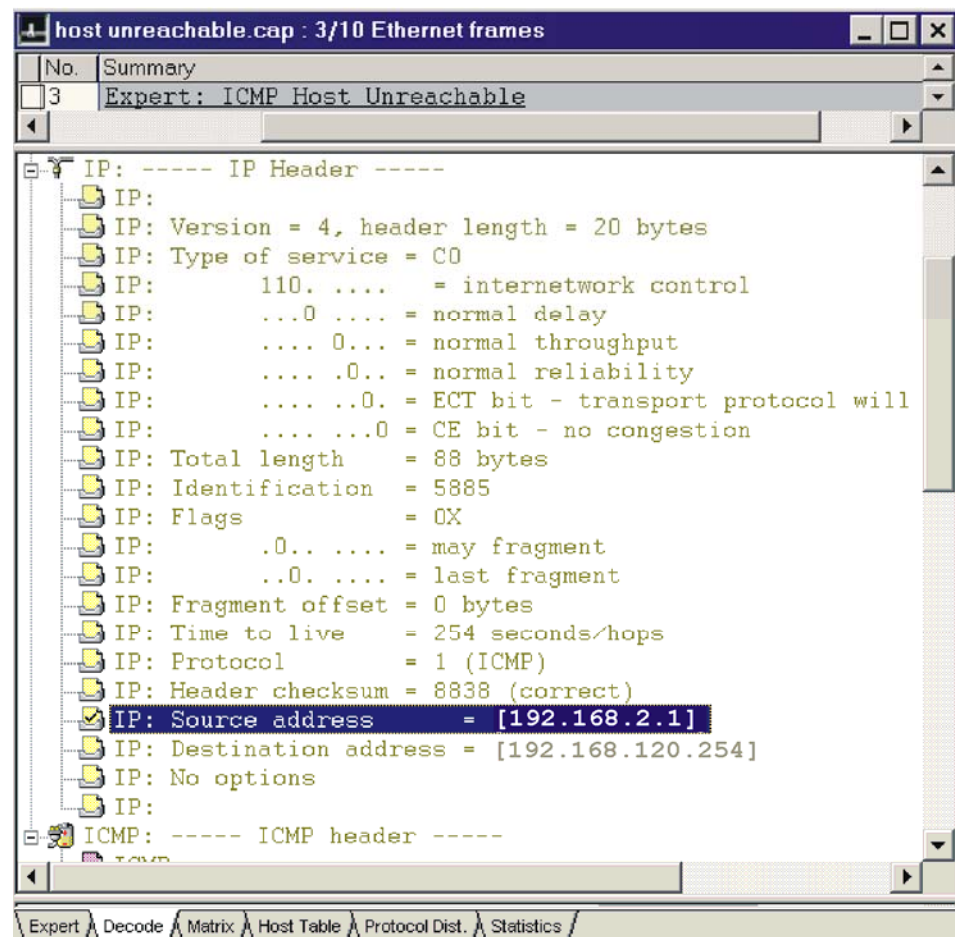



Figura 11-4: Endereço IP do roteador que gerou a mensagem ICMP de destino inalcançável.

Vamos ver um exemplo: suponha que você capturou mensagens ICMP de porta inalcançável originadas na máquina 192.168.5.100 e destinadas à máquina 192.168.1.200. Isto significa que um processo na máquina 192.168.1.200 tentou se comunicar com uma porta desativada da máquina 192.168.5.100. Mas, que porta é esta? Crie um filtro no analisador que selecione apenas datagramas que envolvam as máquinas 192.168.1.200 e 192.168.5.100. É possível que a máquina 192.168.1.200 tente novamente acessar o serviço desativado da máquina 192.168.5.200.

Capture algumas dezenas de quadros. Veja a porta destino das mensagens que precedem uma mensagem ICMP de porta inalcançável. Analisando os quadros capturados você poderá descobrir que porta está desativada na máquina que está gerando as mensagens ICMP de porta inalcançável.

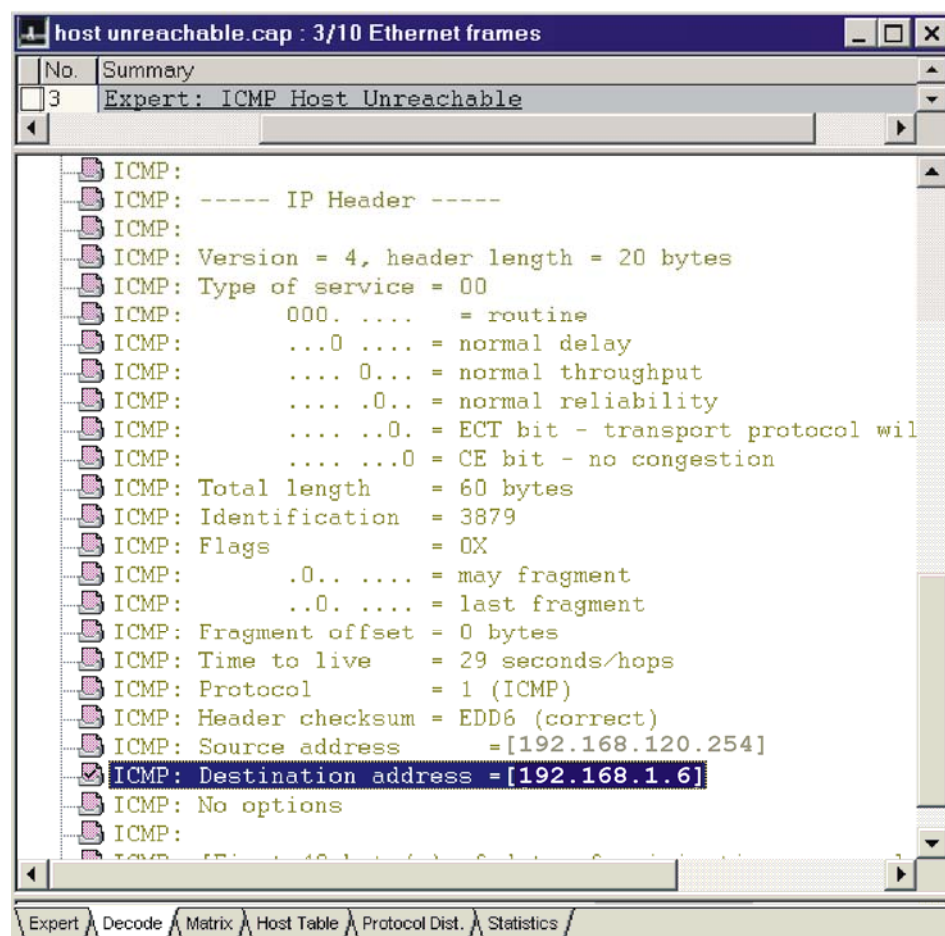



Figura 11-5: Cabeçalho IP do datagrama que causou o envio da mensagem ICMP de destino inalcançável.

Note que se a máquina 192.168.1.200 fizer uma tentativa de comunicação com uma porta inalcançável da máquina 192.168.5.100 e depois desistir, nada poderemos concluir com este teste. Além disso, se as máquinas 192.168.5.100 e 192.168.1.200 estão se comunicando através de vários processos em várias portas distintas, devemos tomar cuidado para não tirar conclusões erradas. Por exemplo, a máquina 192.168.5.100 é servidora Web e de correio eletrônico. Um cliente na máquina 192.168.1.200 está usando estes dois serviços oferecidos pela máquina 192.168.5.100, além de estar tentando acessar nesta um serviço não

ativado. Neste caso, devemos analisar bem a comunicação entre as duas máquinas antes de identificar com certeza que porta está desativada.

11.11 Verificando se pacotes estão sendo descartados por falta de rotas

Neste procedimento descreveremos como verificar se os roteadores da rede estão descartando muitos datagramas por não encontrarem uma rota que possa levá-los ao seu destino.

11.11.1 Descrição e dicas

A variável ipOutNoRoutes da MIB-2 [RFC1213] é do tipo contador. Quando um roteador recebe um datagrama e nenhuma rota que o leve ao destino especificado é encontrada, o datagrama é descartado e a variável ipOutNoRoutes é incrementada.

O crescimento da variável ipOutNoRoutes não é necessariamente um problema de roteamento. Segundo a definição desta variável, quando todos os roteadores *default* de um roteador estão inacessíveis, esta variável também é incrementada. Neste caso, o problema não é de roteamento.

O crescimento desta variável em roteadores que não possuem rota *default* é preocupante e pode indicar erros na tabela de rotas do roteador. O incremento desta variável pode também indicar ataques. Programas maliciosos e *worms*, por exemplo, geram endereços destino falsos, muitas vezes de redes que não existem. O crescimento desta variável em roteadores que deveriam ter rota *default* indica que a rota *default* não está configurada no momento (se ela for aprendida dinamicamente) ou que todos os roteadores *default* não estão acessíveis.

11.11.2 Usando uma estação de gerência SNMP

Recupere o valor da variável ipOutNoRoutes da MIB-2 nos roteadores de sua rede usando uma estação de gerência SNMP. Lembre-se que ela é um contador, e, portanto, o incremento desta variável em um determinado intervalo de tempo é que tem significado. Na maior parte do tempo esta variável não deve mudar de valor.

11.11.3 Usando uma interface de linha de comando

Nesta seção veremos como obter o valor da variável ipOutNoRoute usando uma interface de linha de comando em roteadores Cisco.

Em roteadores Cisco com versão de IOS superior a 10.0 você pode obter estatísticas de tráfego IP com o seguinte comando:

```
roteador> show ip traffic
```

```
IP statistics:
  Rcvd:  2593286165 total, 10600762 local destination
         0 format errors, 0 checksum errors, 885818 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 32532 with options
  Opts:  72 end, 1 nop, 4 basic security, 0 loose source route
         0 timestamp, 0 extended security, 3 record route
         0 stream ID, 0 strict source route, 32459 alert, 0 cipso
         0 other
  Frags: 0 reassembled, 1 timeouts, 226 couldn't reassemble
         496166 fragmented, 0 couldn't fragment
  Bcast: 58033 received, 12 sent
  Mcast: 1893437 received, 3482544 sent
  Sent:  17569897 generated, 1571770454 forwarded
  Drop:  811982 encapsulation failed, 0 unresolved, 0 no adjacency
         10070563 no route, 0 unicast RPF, 0 forced drop
```
(...)

O contador *no route* (em negrito) indica quantos pacotes foram jogados fora devido à falta de rotas. Lembre-se que o valor único de *no route* nada significa. O que vale é o seu incremento no tempo. No exemplo acima vemos que 10070563 datagramas foram descartados por falta de rotas. Este número nada significa. Ele pode ter sido incrementado em um momento em que todos os roteadores *default* estavam inoperantes. Apenas se esta variável estiver crescendo no momento e todos os roteadores *default* estiverem operacionais é que podemos concluir que existe um problema.

11.12 Analisando a origem do tráfego de difusão em um domínio de difusão

Neste procedimento apresentaremos como identificar as máquinas que estão enviando quadros de difusão em um determinado domínio de difusão.

11.12.1 Descrição e Dicas

Antes de entenderemos este procedimento, é necessário sabermos um pouco mais sobre quadros e datagramas de difusão e domínios de difusão.

Existem dois tipos de difusão: difusão nível 2 (enlace) e difusão nível 3 (rede), também chamada difusão lógica. Quadros de difusão nível 2 são destinados ao endereço físico (MAC) de difusão, que é FFFFFFFFFFFF. Quadros ARP são exemplos de quadros de difusão nível 2. Eles são quadros gerados por protocolos da camada de enlace, e não carregam, portanto, dados do protocolo IP ou superiores. Um quadro de difusão nível 3, por sua vez, carrega um datagrama IP cujo endereço destino é o endereço de difusão dirigida ou o endereço de difusão limitada.

O endereço de difusão dirigida é formado pelo prefixo da rede seguido de bits 1 em substituição ao sufixo de identificação da máquina. Por exemplo, o endereço de difusão dirigida da rede 192.168.1.0/24 é 192.168.1.255. Um datagrama de difusão dirigida é roteado até a rede destino como se fosse um datagrama direcionado a uma única máquina desta rede. Quando este quadro chega no

roteador ligado diretamente a esta rede, ele trata de entregar o quadro a todas as máquinas da rede. Para enviar um datagrama de difusão dirigida a origem deve conhecer o prefixo da rede a ser alcançada.

Segundo [BCP0034], roteadores devem ser, por *default*, proibidos de repassar datagramas destinados ao endereço de difusão dirigida. Esta prática foi adotada por questões de segurança, pois datagramas destinados a endereços de difusão dirigida podem ser usados em diversos tipos de ataques de negação de serviço. Assim, um roteador só deve receber um datagrama destinado a um endereço de difusão dirigida se ele tiver sido explicitamente configurado pelo administrador da rede para aceitar rotear este tipo de datagrama. Roteadores mais novos já se comportam assim. Já roteadores mais antigos ainda podem estar repassando datagramas de difusão dirigida e você deve reconfigurá-lo apropriadamente para que ele não mais aceite receber este tipo de tráfego.

O endereço IP 255.255.255.255 é chamado de endereço de difusão limitada. Quando uma estação gera um datagrama destinado a este endereço, todas as estações da mesma rede local que a remetente recebem o datagrama. Datagramas de difusão limitada não são roteados, eles são gerados e entregues em um mesmo domínio de difusão.

Em geral, domínios de difusão são limitados por roteadores ou por VLANs. Tipicamente, as máquinas de um mesmo domínio de difusão compartilham de um mesmo prefixo e máscara de rede. De posse da documentação da rede devemos estar aptos a identificar o prefixo e a máscara de rede de um domínio de difusão.

Em um domínio de difusão onde todos os roteadores negam receber mensagens destinadas ao endereço de difusão dirigida, devemos encontrar apenas quadros de difusão originados em máquinas do domínio de difusão em questão. Suponha que as máquinas de um certo domínio de difusão possuem os seguintes prefixo e máscara de rede: 192.168.2 e 255.255.255.0. Se todos os roteadores ligados diretamente a esta rede negam transmitir quadros de difusão dirigida, encontraremos neste domínio de difusão apenas quadros de difusão originados por máquinas cujo prefixo de rede e máscara de rede são respectivamente 192.168.2 e 255.255.255.0.

Alguns problemas de rede relacionados a VLANs (que definem domínios de difusão) podem causar uma desordem geral nos domínios de difusão da rede. Esta desordem será claramente percebida: encontraremos em um domínio de difusão quadros de difusão nível 2 ou difusão lógica limitada enviados por máquinas que, devido a seu endereço IP, não deveriam estar fazendo parte deste domínio de difusão.

11.12.2 Usando um analisador de protocolos

A única forma de descobrir a origem dos quadros de difusão que trafegam em um domínio de difusão é usando um analisador de protocolos. Nesta seção veremos como este estudo pode ser feito.

Como queremos analisar apenas quadros de difusão, basta conectar o analisador de forma que ele participe do domínio de difusão que deve ser estudado. Seja em um repetidor, seja em um comutador, o analisador receberá todos os quadros de difusão deste domínio de difusão.

Em redes Ethernet, endereços de difusão lógicos sempre são mapeados para o endereço de difusão físico FFFFFFFFFFFF quando vão ser entregues aos destinos finais. Assim, quando uma estação gera um datagrama destinado ao endereço 255.255.255.255, por exemplo, o endereço destino físico do quadro que carrega este datagrama será FFFFFFFFFFFF.

Crie um filtro de captura que selecione apenas quadros de difusão nível 2 para a captura, isto é, quadros cujo endereço MAC destino é FFFFFFFFFFFF. No analisador de protocolos Sniffer, da Network Associates, este filtro pode ser criado como descrito no **UTILIZANDO UM ANALISADOR DE PROTOCOLOS**.

Selecione o filtro criado e capture quadros durante alguns minutos. Em seguida, analise os quadros de difusão capturados. Verifique em o endereço das máquinas que estão enviando quadros de difusão. Se o quadro sendo analisado for um quadro de difusão lógica, olhe o endereço de quem o transmitiu no cabeçalho do datagrama IP (IP fonte). Se o quadro não traz dados do protocolo IP, como ARP, por exemplo, o endereço do remetente estará nos dados do protocolo nível 2. Na Figura 11-6 destacamos o endereço IP da máquina que transmitiu um quadro de difusão ARP. Não será possível localizar o endereço origem de mensagens DHCPDISCOVER – que são enviadas para o endereço destino 255.255.255.255 – pois a máquina que o transmite ainda não sabe qual é o seu próprio endereço IP, por isto mesmo está solicitando um ao servidor DHCP.

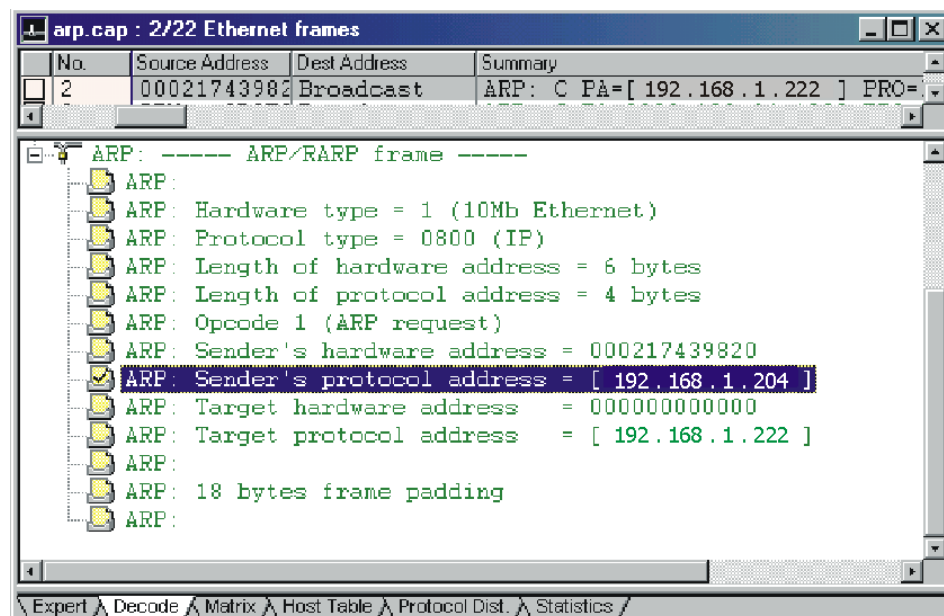



Figura 11-6: Decodificação de uma requisição ARP no Sniffer.

11.13 Analisando a configuração de rede em um hospedeiro

Neste procedimento mostraremos como analisar a configuração de rede – endereço IP, máscara de rede, roteador *default* e servidor de nomes – em um hospedeiro.

11.13.1 Descrição e dicas

A configuração de rede de um hospedeiro normalmente envolve os seguintes valores:

- endereço IP do hospedeiro;
- máscara de rede;
- endereço IP dos servidores de nomes de domínio;
- endereço IP do roteador *default*.

A partir do endereço IP, da máscara de rede e do endereço do roteador *default*, uma pequena – mas imprescindível – tabela de rotas é criada.

Estas configurações podem ser obtidas dinamicamente pelo hospedeiro ou podem ser definidas nele manualmente. No primeiro caso diz-se que o hospedeiro tem IP dinâmico, pois é um cliente DHCP, e no segundo que ele tem IP estático.

Verificar as configurações de rede em hospedeiros é uma tarefa bastante simples. Os próprios sistemas operacionais oferecem ferramentas que nos permitem visualizar as configurações de rede do hospedeiro.

11.13.2 Usando outras ferramentas de gerência

Veremos nesta seção como obter as configurações básicas de rede em máquinas com sistema operacional Windows e Linux.

Em máquinas Windows 98/ME/NT/2000 o comando `ipconfig /All` pode ser utilizado. Veja o exemplo da saída deste comando na Figura 11-7. Exceto no Windows NT/2000, o comando `winipcfg` também pode ser utilizado. A Figura 11-8 apresenta o resultado deste comando.

Os comandos já apresentados informam o endereço IP do roteador *default* configurado em um hospedeiro. Se você deseja analisar a tabela de rotas completa de uma máquina com sistema operacional Windows execute o seguinte comando a partir de um *prompt* de comandos:

```
C:\> route print
```

```
Prompt de comando
                                                  192.168.1.54

C:\WINDOWS>ipconfig /all

Configuração de IP do Windows

        Nome do host . . . . . . . . . . . . : pc-1.exemplo.com.br
        Sufixo DNS primário. . . . . . . . . :
        Tipo de nó . . . . . . . . . . . . . : Difusão
        Roteamento de IP ativado . . . . . . : não
        Proxy WINS ativado . . . . . . . . . : não

Adaptador Ethernet Conexão local:

        Sufixo DNS específico de conexão  . . : exemplo.com.br
        Descrição . . . . . . . . . . . . . . : SiS 900 PCI Fast Ethernet Adapter
        Endereço físico . . . . . . . . . . . : 00-07-95-15-F3-E8
        DHCP ativado. . . . . . . . . . . . . : Não
        Endereço IP . . . . . . . . . . . . . : 192.168.1.1
        Máscara de sub-rede . . . . . . . . . : 255.255.255.0
        Gateway padrão. . . . . . . . . . . . : 193.168.1.254
        Servidores DNS. . . . . . . . . . . . : 192.168.1.53
                                                192.168.1.54

C:\WINDOWS>
```

Figura 11-7: Exemplo do resultado do comando ipconfig /All.

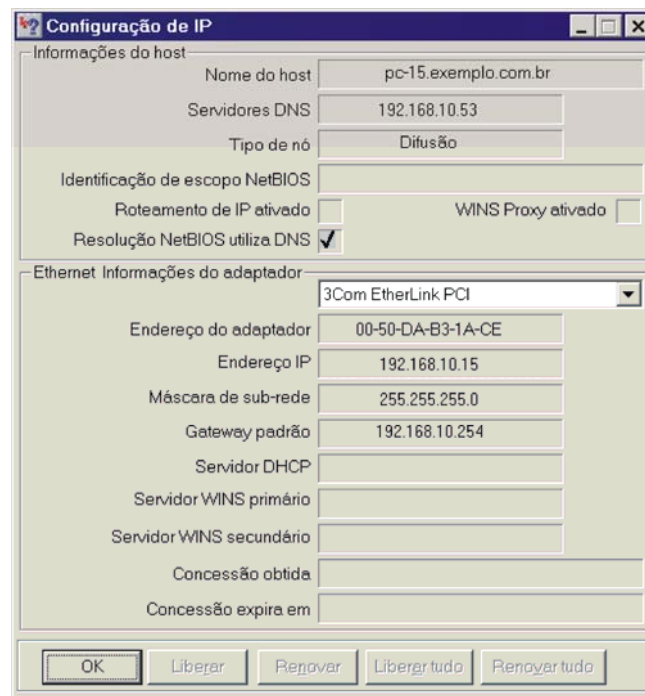



Figura 11-8: Saída do comando winipcfg.

Em máquinas Linux esta verificação será um pouco mais trabalhosa. Para descobrir o endereço IP do hospedeiro e a máscara de sub-rede execute o seguinte comando:

```
[maria@pc-15~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:04:AC:4C:98:DF
          inet      addr:192.168.10.15              Bcast:192.168.10.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9103385 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8066438 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2151783033 (2052.1 Mb)  TX bytes:439771715 (419.3 Mb)
```

```
          Interrupt:15 Base address:0x2180

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:788372 errors:0 dropped:0 overruns:0 frame:0
          TX packets:788372 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:111515980 (106.3 Mb)  TX bytes:111515980 (106.3 Mb)
```

O comando a seguir apresenta a tabela de rotas do hospedeiro. Observe o roteador *default* configurado.

[maria@pc-15~]$ route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.22.32	192.168.10.131	255.255.255.255	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	**192.168.10.254**	**0.0.0.0**	**UG**	**0**	**0**	**0**	**eth0**

Quando o hospedeiro recebe mensagens ICMP de redirecionamento, ele pode adicionar em sua tabela de roteamento rotas específicas para hospedeiros. Na segunda linha da tabela de rotas apresentada acima, por exemplo, vemos uma rota específica para outro hospedeiro (192.168.22.32). As mensagens ICMP de redirecionamento ensinam rotas melhores aos hospedeiros e estas rotas são inseridas na tabela de rotas (ver Seção 11.8.1). Idealmente, um hospedeiro não deve receber mensagens de redirecionamento e a existência de rotas específicas para outros hospedeiros em tabelas de rotas só deveria ser constatada caso a rota tenha sido adicionada manualmente pelo administrador da rede.

O nome do hospedeiro pode ser visualizado através do seguinte comando:

```
# hostname –fqdn
pc-15.exemplo.com.br
```

Por fim, para ver quais os servidores DNS configurados para responder consultas DNS deste hospedeiro veja o arquivo /etc/resolv.conf.

```
# more /etc/resolv.conf
```

domain exemplo.com.br

nameserver 192.168.1.53

nameserver 192.168.1.54

nameserver 192.168.1.55

A diretiva `domain` indica o domínio de nomes a que o hospedeiro pertence. As diretivas `nameserver` informam os endereços IP dos servidores de nomes deste hospedeiro, que serão consultados na ordem em que foram configurados no arquivo.

11.14 Verificando conectividade via IP e conectividade via nome de domínio

Neste procedimento veremos como identificar se a falta de conectividade para um determinado equipamento é total ou se apresenta apenas quando o seu nome de domínio é usado.

11.14.1 Descrição e Dicas

Em várias ocasiões, nos deparamos com problemas reportados como falta de conectividade. Uma rede existe para que seus serviços possam ser utilizados pelos usuários. Em geral, estes serviços são acessados através dos nomes das máquinas onde estão instalados os programas servidores. Quando o mapeamento dos nomes dos servidores para endereços IP não é possível, os usuários têm a impressão de que o serviço não está disponível ou que a rede não está funcionando.

A realização do teste proposto neste procedimento é indicado quando desconfiamos que o problema está no serviço de nomes e não em camadas inferiores.

11.14.2 Usando ping

Nesta seção mostramos como usar o ping para confirmar problemas com o serviço de nomes.

Suponha que a sua estação de gerência se comunica com os elementos gerenciados através de seus nomes de domínio. De repente, você percecebeu que a partir de um certo ponto, todos os elementos da rede ficaram não operacionais. Você desconfia que o problema é com o serviço de nomes, então resolve fazer um teste simples para confirmar ou negar sua suspeita. O teste consiste em escolher um endereço IP de um equipamento que, de acordo com a estação, não está acessível. Você escolheu o equipamento roteador23.exemplo.com.br, cujo endereço IP é 192.168.23.3. Simplesmente envie ping para este equipamento primeiro usando seu IP e depois seu nome. Veja o resultado:

```
# ping 192.168.23.3
PING 192.168.23.3 (192.168.23.3): 56 data bytes
64 bytes from 192.168.23.3: icmp_seq=0 ttl=255 time=1.0 ms
64 bytes from 192.168.23.3: icmp_seq=1 ttl=255 time=0.6 ms
64 bytes from 192.168.23.3: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 192.168.23.3: icmp_seq=3 ttl=255 time=0.6 ms
64 bytes from 192.168.23.3: icmp_seq=4 ttl=255 time=0.6 ms

--- 192.168.23.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/1.0 ms
# ping roteador23.exemplo.com.br
```

Note que o equipamento respondeu quando você usou seu endereço IP, mas não o seu nome. Este é um comportamento típico de uma rede com problemas no serviço DNS.

11.15 Referências

11.15.1 Recursos online (Internet)

[ANALYZING-DHCP-LOG] *Analyzing Server Log files*. Microsoft Windows 2000 Server Documentation.

http://www.microsoft.com/windows2000/en/server/help/sag_DHCP_tro_AnalyzingSrvLogs.htm

[WIN-TIP316] *Tip #316: Enable DHCP Logging*.

http://windows.about.com/library/tips/bltip316.htm

[WIN-TIP412] *Tip #412: DHCP Logging Event IDs*.

http://windows.about.com/library/tips/bltip412.htm

11.15.2 RFCs

[BCP0034] Senie, ,D. Changing the Default for Directed Broadcasts in Routers. Agosto, 1999.

[RFC 792] Postel, J. Internet Control Message Protocol. Setembro, 1981

[RFC1122] Braden, R. Requirements for Internet Hosts - Communication Layers. Outubro, 1989

[RFC1812] Baker, F. Requirements for IP Version 4 Routers. Junho, 1995.

[RFC1213] McCloghrie, K., Rose, M. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Março, 1991.

[RFC2096] Baker, F. IP Forwarding Table MIB. Janeiro, 1997.

[RFC2131] Droms, R. Dynamic Host Configuration Protocol. 1997.

11.15.3 Livros base

[COMER] Comer, D. Internetworking with TCP/IP: Principles, Protocols, and Architectures. Volume 1. Quarta edição. Prentice Hall, 2000.

Capítulo 12

12 Procedimentos referenciados nos problemas de nível de aplicação

Neste capítulo apresentamos 8 procedimentos que informam como obter e analisar informações de gerência. Os procedimentos apresentados neste capítulo informam como obter os sinais que foram mais referenciados nos problemas de nível de aplicação. No entanto, existem alguns problemas de outras camadas que podem lhes referenciar.

12.1 Verificando consistência de dados nos servidores DNS primário e secundários

Nesta seção veremos como verificar se servidores primário e secundários respondem igualmente às mesmas consultas, isto é, se eles possuem os mesmos dados sobre as zonas pelas quais respondem.

12.1.1 Descrição e dicas

O servidor de nomes primário de uma zona recupera as configurações de nomes de sua zona a partir de um arquivo local. Já os servidores secundários recuperam os dados sobre a zona a partir de outro servidor DNS, chamado o servidor principal. Geralmente, os servidores secundários recuperam dados sobre a zona a partir do servidor primário. Não é comum, mas é também possível que servidores secundários recuperem os dados da zona a partir de outro servidor secundário.

Os servidores de nomes primário e secundários devem retornar a mesma resposta quando uma mesma consulta lhes é feita. Suponha que ns1.exemplo.com.br é o servidor primário do domínio exemplo.com.br. Os servidores ns2.exemplo.com.br e ns3.exemplo.com.br são servidores secundários que obtêm os dados sobre a zona exemplo.com.br a partir de ns1. Quando perguntarmos a ns1, ns2 e ns3 qual o IP correspondente ao nome www.exemplo.com.br, todos os servidores devem oferecer a mesma resposta.

Os servidores de nomes mais novos (BIND versões 8.2.3 e superiores e servidor DNS do Windows 2000, por exemplo) notificam por *default* os servidores secundários quando percebem que os seus arquivos de zonas foram modificados. Quando o servidor principal age desta forma, as modificações em arquivos de zonas são rapidamente vistas pelos servidores secundários. Quando

o servidor principal não notifica os secundários sobre modificações nos arquivos de zonas, os servidores secundários só perceberão a mudança após algum tempo, que é no máximo o intervalo de *refresh* configurado no registro SOA do arquivo de zonas modificado. Portanto, se seus servidores principais não notificam os servidores secundários sobre mudanças, as respostas de servidores principais e secundários podem diferir durante algum tempo (no máximo o intervalo de *refresh*) – isso é normal.

12.1.2 Usando nslookup, dig e host

Descreveremos nesta seção como verificar a consistência dos dados entre servidores DNS primário e secundários usando as seguintes ferramentas: `nslookup`, `dig` e `host`.

Antes de realizar este procedimento você terá que decidir quais as consultas que serão feitas aos servidores primário e secundários. Você deve consultar os servidores de nomes primário e secundários sobre as últimas modificações realizadas no servidor de nomes primário. Suponha que a última modificação realizada foi alterar o IP da máquina www.exemplo.com.br de 192.168.1.2 para 192.168.1.80. Então, solicite aos servidores de nomes primário e secundários que façam o mapeamento direto e reverso de www.

Conecte-se em um dos servidores de nomes que serão testados. O servidor de nomes que, por *default*, responderá às consultas feitas através de `nslookup`, `dig` ou `host` é o servidor DNS que serve à máquina onde você está conectado. Se esta máquina abriga um servidor DNS é bastante provável que ela seja cliente DNS dela mesma.

No exemplo mostrado a seguir o comando `nslookup` foi utilizado. Quando este comando é executado sem parâmetros ele age de forma interativa. Estabelecemos conexão com o servidor DNS primário do domínio exemplo.com.br, que é ns1.exemplo.com.br e executamos os seguintes comandos:

```
[maria@ns1 ~]$ nslookup
> www.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   www.exemplo.com.br
Address: 192.168.1.80
> 192.168.1.80
Server:         192.168.1.53
Address:        192.168.1.53#53

80.1.168.192.in-addr.arpa      name = www.exemplo.com.br.
>
```

Com estas consultas, descobrimos que, no servidor de nomes primário, a máquina cujo nome é www.exemplo.com.br possui o endereço IP 192.168.1.80 e a máquina cujo IP é 192.168.1.80 tem o nome www.exemplo.com.br. Uma perfeita correspondência de registros A e PTR. Os resultado foi o que esperávamos.

Agora devemos realizar esta mesma consulta nos servidores secundários de exemplo.com.br. O objetivo é verificar se os servidores secundários também consideram o mapeamento www.exemplo.com.br ⇔ 192.168.1.80. Usando ainda o `nslookup` no modo interativo em ns1 (continuação dos comandos apresentados anteriormente), execute os comandos a seguir:

```
> server ns2.exemplo.com.br
Default server: ns2.exemplo.com.br
Address: 192.168.1.54#53
> www.exemplo.com.br
Server:         ns2.exemplo.com.br
Address:        192.168.1.54#53

Name:   www.exemplo.com.br
Address: 192.168.1.2
> 192.168.1.80
Server:         ns2.exemplo.com.br
Address:        192.168.1.54#53

** server can't find 80.1.168.192.in-addr.arpa.: NXDOMAIN
> 192.168.1.2
Server:         ns2.exemplo.com.br
Address:        192.168.1.54#53

2.1.168.192.in-addr.arpa      name = www.exemplo.com.br.
> server ns3.exemplo.com.br
Default server: ns3.exemplo.com.br
Address: 192.168.1.55#53
> www.exemplo.com.br
Server:         ns3.exemplo.com.br
Address:        192.168.1.55#53

Name:   www.exemplo.com.br
Address: 192.168.1.2
> 192.168.1.80
Server:         ns3.exemplo.com.br
Address:        192.168.1.55#53

** server can't find 80.1.168.192.in-addr.arpa.: NXDOMAIN
```

```
> 192.168.1.2
Server:         ns3.exemplo.com.br
Address:        192.168.1.55#53

2.1.168.192.in-addr.arpa      name = www.exemplo.com.br.
```

O comando `server <nome do servidor DNS>` é utilizado para modificar o servidor que responde às consultas realizadas com `nslookup`. Com estas consultas, descobrimos que os dados dos servidores secundários não estão compatíveis com os dados do servidor primário. No servidor primário o endereço IP de www.exemplo.com.br é 192.168.1.80, enquanto que nos servidores secundários o endereço IP de www ainda é 192.168.1.2.

A ferramenta `nslookup` é automaticamente instalada quando o servidor de nomes BIND ou do Windows é instalado. Portanto, este procedimento pode ser realizado em quaisquer destes servidores.

Outra ferramenta que pode lhe ajudar se o seu servidor DNS for uma implementação BIND é o `dig`. Para realizar as mesmas consultas que acabamos de fazer com `nslookup` conecte-se em ns1 e execute os seguintes comandos:

```
maria@ns1:~$ dig www.exemplo.com.br

maria@ns1:~$ dig –x 192.168.1.80
```

Assim como o `nslookup`, o `dig` também usa, por *default*, o servidor de nomes configurado para servir a máquina onde ele está sendo executado. Com os comandos apresentados, você vai descobrir como www está configurado em ns1. Vai descobrir que para ns1 o IP de www é 192.168.1.80. A saída do `dig` oferece muito mais informações que a saída do `nslookup`. Veja, por exemplo, a resposta do dig para a consulta dig www.exemplo.com.br:

```
maria@ns1:~$ dig www.exemplo.com.br

; <<>> DiG 9.2.0rc3 <<>> www.exemplo.com.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45099
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.exemplo.com.br.          IN      A

;; ANSWER SECTION:
www.exemplo.com.br.   86400   IN      A       192.168.1.80

;; AUTHORITY SECTION:
exemplo.com.br.          86400   IN      NS      ns1.exemplo.com.br.

;; ADDITIONAL SECTION:
ns1.exemplo.com.br.  86400   IN      A       192.168.1.53
```

```
;; Query time: 1 msec
;; SERVER: 192.168.1.53#53(192.168.1.53)
;; WHEN: Tue Mar 12 20:38:41 2002
;; MSG SIZE  rcvd: 137
```

Em negrito destacamos a resposta que estávamos procurando. Até agora consultamos apenas o servidor primário (ns1). Para realizar consultas nos demais servidores a partir de ns1 execute os seguintes comandos:

```
maria@ns1:~$ dig @ns2.exemplo.com.br www.exemplo.com.br

maria@ns1:~$ dig @ns2.exemplo.com.br –x 192.168.1.80

maria@ns1:~$ dig @ns3.exemplo.com.br www.exemplo.com.br

maria@ns1:~$ dig @ns3.exemplo.com.br –x 192.168.1.80
```

Existe ainda uma outra ferramenta que pode ser usada para realizar consultas DNS: é a ferramenta `host`. Execute os comandos a seguir para realizar as mesmas consultas que realizamos anteriormente com `nslookup` e `dig`:

```
maria@ns1:~$ host www.exemplo.com.br

maria@ns1:~$ host 192.168.1.80

maria@ns1:~$ host www.exemplo.com.br ns2.exemplo.com.br

maria@ns1:~$ host 192.168.1.80 ns2.exemplo.com.br

maria@ns1:~$ host www.exemplo.com.br ns3.exemplo.com.br

maria@ns1:~$ host 192.168.1.80 ns3.exemplo.com.br
```

Veja um exemplo da resposta deste comando:

```
maria@ns1:~$ host 192.168.1.80

80.1.168.192.in-addr.arpa domain name pointer www.exemplo.com.br.
```

12.2 Analisando mensagens de *log* do servidor DNS BIND

Neste procedimento vamos falar um pouco sobre mensagens de *log* do servidor DNS implementação BIND.

12.2.1 Descrição e Dicas

Um bom gerente de redes deve estar sempre atento aos arquivos de *logs* de seus servidores. Nestes arquivos encontramos informações importantes sobre o estado dos serviços.

Mostraremos neste procedimento apenas duas mensagens que podem surgir no arquivo de *logs* do servidor DNS, mas muitas outras mensagens certamente

estarão presentes. É interessante que você entenda estas mensagens, pois elas podem indicar algum problema.

12.2.2 Verificando logs do servidor DNS

Mostraremos nesta seção onde se localiza o arquivo de *logs* do servidor DNS (BIND) e algumas mensagens escritas neste arquivo em situações de erro. Muitas outras informações sobre mensagens de *logs* do servidor DNS podem ser encontradas em [DNS&BIND].

A implementação BIND do serviço DNS enviará mensagens para o arquivo de *log* através do `syslog`. Por *default*, as mensagens de *log* do DHCP serão encontradas juntamente com mensagens de *logs* de todos os outros *daemons* que também usam o `syslog`. Tipicamente estas mensagens são encontradas em /var/log/messages ou /var/adm/messages, dependendo do seu sistema.

Se você modificou a configuração *default* do syslogd, veja no arquivo /etc/syslog.conf em que arquivo as mensagens de *logs* dos *daemons* estão sendo geradas.

O arquivo que contém *logs* do BIND é um arquivo de texto ASCII.

Para ver todo o arquivo de *logs*:

```
# more /var/logs/messages
```

Para ver apenas as últimas 50 linhas do arquivo:

```
# tail –n 50 /var/logs/messages
```

Para localizar a palavra TTL, por exemplo:

```
# grep TTL /var/logs/messages
```

TTL *DEFAULT* NÃO CONFIGURADO

Em servidores DNS BIND versões 8.2 e superiores, o TTL *default* de uma zona deve ser configurado explicitamente através da diretiva $TTL. Quando isto não for feito o servidor DNS escreverá uma mensagem no arquivo de *log* indicando o erro. A mensagem a seguir pode ser encontrada no arquivo de *logs* do servidor DNS BIND versão 8:

Apr 13 21:40:39 ns1 named[68]: Zone "exemplo.com.br" (file exemplo.zone): no default TTL ($TTL <value>) set, using SOA minimum instead

Já em servidores DNS BIND versão 9 a mensagem é um pouco diferente. Veja abaixo:

Apr 13 21:40:39 ns1 named[68]: dns_zone_load: zone exemplo.com.br/IN: database exemplo.zone: dns_db_load failed: no TTL

SERVIDOR PRINCIPAL INALCANÇÁVEL

No arquivo de *logs* de servidores DNS secundários podemos encontrar mensagens que indicam que não foi possível alcançar o servidor principal ao tentar realizar uma transferência de zona. Nos servidores DNS BIND versões 4 e 8 a mensagem é a seguinte:

Apr 13 21:40:39 ns1 named[68]: zoneref: Masters for secondary zone "exemplo.com.br" unreachable

Em servidores BIND versão 9 a mensagem é como segue:

```
Apr 13 21:40:39 ns1 named[68]: refresh_callback: zone exemplo.com.br/IN: failure for 192.168.1.53#53: timed out
```

SOBRE LOGS DO SERVIDOR DNS WINDOWS

As mensagens de log do servidor DNS do Windows podem ser vistas através do Visualizador de Eventos. Pressione Iniciar > Programas > Ferramentas Administrativas > Visualizador de Eventos e em seguida clique em Servidor DNS para ver apenas as mensagens deste servidor. O servidor DNS da Microsoft pode ser configurado para escrever outras mensagens de *logs* em um arquivo. Este arquivo localiza-se por *default* em %Raiz do sistema%\System32\dns. Ele se chama Dns.log e pode ser lido no `WordPad` (arquivo escrito no formato RTF).

12.3 Verificando a resolução de nomes de domínio externos

Neste procedimento apresentaremos como verificar se um servidor de nomes está resolvendo nomes de domínios externos.

12.3.1 Descrição e Dicas

Em geral, quando solicitamos a um servidor de nomes que ele resolva nomes de domínios externos, uma das seguintes situações ocorrerá:

- o servidor de nomes já resolveu esta requisição e a resposta ainda está armazenada em cache. Então, o servidor simplesmente envia a resposta ao cliente DNS;

- o servidor DNS não possui a resposta desta consulta armazenada em cache e precisa falar com outros servidores, que podem estar dentro ou fora da organização.

Quando um servidor DNS não conseguir se comunicar com outros servidores DNS — os servidores DNS raiz, por exemplo — nomes de domínios externos não poderão ser resolvidos.

Suponha que ns1.exemplo.com.br seja servidor primário de uma única zona: exemplo.com.br. Se, por algum motivo, ns1 não conseguir se comunicar com pelo menos um servidor raiz, apenas nomes do domínio exemplo.com.br poderão ser resolvidos por ele. Ele não será capaz de responder qualquer consulta que envolva outro domínio.

12.3.2 Usando nslookup, dig e host

Nesta seção apresentaremos como podemos verificar se um servidor de nomes está resolvendo nomes de domínios externos. Para tal usaremos as ferramentas `nslookup`, `dig` e `host`.

Conecte-se no servidor de nomes que você deseja testar. O servidor de nomes que, por *default*, responderá as consultas feitas através de `nslookup`, `dig` ou

`host` é o servidor DNS que serve à máquina onde você está conectado. Se esta máquina abriga um servidor DNS é bastante provável que ela seja cliente DNS dela mesma.

Primeiramente, certifique-se de que o servidor de nomes em questão está resolvendo nomes locais apropriadamente. Use `nslookup`, `dig` ou `host` para resolver nomes de máquinas locais. Usaremos como exemplo o servidor ns1.exemplo.com.br, que é o servidor de nomes primário do domínio exemplo.com.br. Sabemos que este servidor deve saber mapear o nome www.exemplo.com.br para um endereço IP. Então, esta foi a primeira consulta que realizamos.

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup www.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   www.exemplo.com.br
Address: 192.168.1.80
```

Em seguida, escolha um nome de uma máquina um domínio externo. Escolhemos o nome externo www.cisco.com. Veja a seguir as consultas e respectivas respostas:

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup www.cisco.com
Server:         192.168.1.53
Address:        192.168.1.53#53

Non-authoritative answer:
Name:   www.cisco.com
Address: xx.xx.xx.25
```

USANDO DIG

```
maria@ns1:~$ dig www.cisco.com

; <<>> DiG 9.2.0rc3 <<>> www.cisco.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20094
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; ANSWER SECTION:
www.cisco.com.          86400   IN      A       xx.xx.xx.25

;; AUTHORITY SECTION:
cisco.com.              86400   IN      NS      ns1.cisco.com.
cisco.com.              86400   IN      NS      ns2.cisco.com.

;; Query time: 908 msec
;; SERVER: 192.168.1.53#53(192.168.1.53)
;; WHEN: Thu Apr 11 10:52:33 2002
;; MSG SIZE  rcvd: 83
```

USANDO HOST

```
maria@ns1:~$ host www.cisco.com
www.cisco.com has address xx.xx.xx.25
```

Nas consultas realizadas, obtivemos sempre resposta do servidor. Veja agora como o servidor responde a estes mesmos comandos quando não consegue, por alguma razão, se comunicar com os servidores raiz:

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup www.cisco.com
Server:         192.168.1.53
Address:        192.168.1.53#53

;; connection timed out; no servers could be reached
```

USANDO DIG

```
maria@ns1:~$ dig www.cisco.com

; <<>> DiG 9.2.0rc3 <<>> www.cisco.com
;; global options:  printcmd
;; connection timed out; no servers could be reached
```

USANDO HOST

```
maria@ns1:~$ host www.cisco.com
;; connection timed out; no servers could be reached
```

Estes são resultados típicos obtidos quando o servidor que está realizando a consulta não obtém respostas de outro servidor após um certo intervalo de tempo. Nestes exemplos, o servidor DNS não pôde resolver as consultas feitas a ele porque, por alguma razão, um dos servidores consultados por ele não pôde ser alcançado.

Quando a consulta realizada não pode ser resolvida porque o nome ou o IP que deve ser mapeado não existe, os comandos nslookup, dig e host respondem com NXDOMAIN ou non existent domain. Veja alguns exemplos:

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup www.exemplp.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

** server can't find www.exemplp.com.br.: NXDOMAIN
```

USANDO DIG

```
maria@ns1:~$ dig www.exemplp.com.br

; <<>> DiG 9.2.0rc3 <<>> www.exemplp.com.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53108
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.exemplp.com.br.            IN      A

;; AUTHORITY SECTION:
com.br.                       10762    IN       SOA      NS.DNS.br.
Hostmaster.REGISTRO.br. 2002041600 7200 3600 604800 86400
```

```
;; Query time: 1 msec
;; SERVER: 200.129.64.130#53(200.129.64.130)
;; WHEN: Tue Apr 16 08:37:22 2002
;; MSG SIZE  rcvd: 99
```

USANDO HOST

```
maria@ns1:~$ host www.exemplp.com.br
Host www.exemplp.com.br. not found: 3(NXDOMAIN)
```

Assim, podemos diferenciar claramente quando não é possível realizar uma consulta porque um dos servidores não responde (TIMED OUT) e quando a resposta a esta consulta realmente não existe (NXDOMAIN).

Se você quiser obter mais detalhes sobre a consulta, pode executar os comandos `nslookup` e `dig` com a opção que faz com que eles ofereçam resultados mais detalhados sobre a consulta. Veja exemplos:

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup -d2 www.cisco.com
main parsing www.cisco.com
(…)
looking up www.cisco.com
setup_system()
got a nameserver line
make_server(192.168.1.53)
(…)
start_lookup()
setup_lookup(0x8161d50)
resetting lookup counter.
(…)
using root origin
recursive query
add_question()
starting to render the message
(…)
send_udp(40123010)
bringup_timer()
have local timeout of 5
working on lookup 0x8161d50, query 0x40123010
(…)
sending a request
(…)
send_done()
(…)
connect_timeout()
(…)
resending UDP request to first server
(…)
sending a request
(…)
;; connection timed out; no servers could be reached
cancel_lookup()
(…)
```

USANDO DIG

O comando dig também aceita a mesma opção `d2`. O comando `dig` correspondente ao comando `nslookup` apresentado anteriormente é:

```
# maria@ns1:~$ dig -d2 www.cisco.com
```

12.4 Analisando tráfego DNS de um servidor de nomes de domínio

Neste procedimento vamos analisar o tráfego de entrada e saída de um servidor DNS usando um analisador de protocolos.

12.4.1 Descrição e Dicas

Analisar o tráfego DNS de entrada e saída de um servidor DNS pode ajudar a descobrir problemas como clientes DNS mal configurados, filtros IP barrando o tráfego DNS e ataques de negação de serviço.

Se, por exemplo, virmos que o servidor envia consultas DNS para outros servidores, mas nunca obtém as respostas, é possível que exista um filtro IP barrando o tráfego entre o servidor DNS em estudo e outros servidores DNS.

Ao analisarmos todo o tráfego de entrada e saída do servidor – e não apenas o tráfego DNS – podemos encontrar outros sinais, como por exemplo mensagens ICMP de porta inalcançável, indicando que o processo servidor não está em execução.

Se nenhum problema existir no servidor DNS e em seus clientes, e se também não existirem filtros barrando o tráfego DNS, veremos basicamente:

- consultas DNS chegando no servidor e as respectivas respostas sendo transmitidas por ele para os emissores das consultas. Em se tratando de um servidor DNS interno, veremos apenas requisições de clientes internos;

- consultas enviadas por este servidor cujo tráfego está sob análise para outros servidores DNS e as respectivas respostas chegando logo mais.

12.4.2 Usando um analisador de protocolos

Nesta seção veremos como analisar o tráfego de um servidor DNS usando um analisador de protocolos. Usaremos o analisador de protocolos Sniffer, da Network Associates, como exemplo.

Conecte o analisador de protocolos de forma que ele capture todo o tráfego do servidor de nomes que você deseja testar. Veja no UTILIZANDO UM ANALISADOR DE PROTOCOLOS dicas de como conectar o analisador.

Depois de conectar o analisador, você pode criar um filtro que capture apenas o tráfego DNS do servidor ou pode capturar todo o tráfego do servidor.

Aconselhamos que inicialmente você capture todo o tráfego e só se perceber que não há nada errado (várias mensagens ICMP sendo enviadas ou transmitidas pelo servidor, por exemplo), se concentrar apenas no tráfego DNS.

Se você perceber que muitas mensagens ICMP estão sendo transmitidas e/ou recebidas pelo servidor DNS analise-as como mostrado nos procedimentos apresentados nas Seções 11.8, 11.9 e 11.10. Basicamente, veja origem, destino e tipo das mensagens ICMP.

Analise o tráfego DNS do servidor. O servidor responde a todas as consultas feitas a ele? Existem consultas sem respostas realizadas pelo servidor? Quem consulta o servidor? É normal que estas máquinas o consultem? Estas são algumas perguntas que você deve responder ao analisar o tráfego DNS do servidor.

Na Figura 12-1 apresentamos uma seqüência de quadros onde o servidor DNS envia consultas para outros servidores, mas não recebe as respectivas respostas.

No.	Stat	Source Address	Dest Address	Summary
1	M	[192.168.1.53]	[143.108.23.2]	DNS: C ID=29729 OP=QUERY NAME=www
2		[192.168.1.53]	[200.255.253.234]	DNS: C ID=4837 OP=QUERY NAME=www.
3		[192.168.1.53]	[192.134.0.49]	DNS: C ID=44788 OP=QUERY NAME=www
4		[192.168.1.53]	[200.19.119.99]	DNS: C ID=22394 OP=QUERY NAME=www
5		[192.168.1.53]	[204.152.184.64]	DNS: C ID=43965 OP=QUERY NAME=www
6		[192.168.1.53]	[143.108.23.2]	DNS: C ID=53188 OP=QUERY NAME=www
7		[192.168.1.53]	[200.255.253.234]	DNS: C ID=45982 OP=QUERY NAME=www
8		[192.168.1.53]	[192.134.0.49]	DNS: C ID=22991 OP=QUERY NAME=www
9		[192.168.1.53]	[200.19.119.99]	DNS: C ID=40054 OP=QUERY NAME=www
10		[192.168.1.53]	[143.108.23.2]	DNS: C ID=10003 OP=QUERY NAME=www
11		[192.168.1.53]	[204.152.184.64]	DNS: C ID=25236 OP=QUERY NAME=www
12		[192.168.1.53]	[200.255.253.234]	DNS: C ID=55424 OP=QUERY NAME=www

Figura 12-1: Servidor DNS envia consultas e não recebe resposta alguma.

12.5 Verificando consistência de mapeamentos DNS direto e reverso

Neste procedimento será descrito como verificar se há descasamento de mapeamento reverso e direto no servidor de nomes primário.

12.5.1 Descrição e dicas

O mapeamento direto informa qual o endereço IP associado a um certo nome de domínio. O mapeamento reverso, como o próprio nome diz, faz o oposto: informa qual o nome de domínio correspondente a um dado endereço IP. Em geral queremos que o mapeamento direto e reverso estejam casados, isto é, que o mapeamento direto de um nome A leve a um dado IP, e o mapeamento reverso deste IP leve ao mesmo nome A.

É possível que nomes de domínio tenham apelidos. Por exemplo, é perfeitamente possível que a máquina cujo nome de domínio é

servidor.exemplo.com.br tenha os seguintes apelidos: ftp.exemplo.com.br e mail.exemplo.com.br. Neste caso, o mapeamento direto vai indicar que o nome é um apelido de outro.

12.5.2 Usando nslookup, dig e host

Nesta seção veremos como verificar se mapeamentos direto e reverso correspondentes são consistentes utilizando as ferramentas `nslookup`, `dig` e `host`.

Suponha que você deseja estudar os mapeamentos diretos e reversos da máquina cliente pc1.exemplo.com.br, cujo IP é 192.168.11.1. Para realizar esta tarefa usando `nslookup` conecte-se no servidor de nomes primário da zona exemplo.com.br e execute os seguintes comandos:

USANDO NSLOOKUP

```
[maria@ns1 ~]$ nslookup
> pc1.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   pc1.exemplo.com.br
Address: 192.168.11.1
> 192.168.11.1
Server:         192.168.1.53
Address:        192.168.1.53#53

1.11.168.192.in-addr.arpa      name = pc-1.exemplo.com.br.
```

Note que o mapeamento reverso de 192.168.11.1 leva ao nome de domínio **pc-1**.exemplo.com.br e não a **pc1**.exemplo.com.br.

É possível também que o mapeamento direto e reverso não casem porque um dos dois não existe. Suponha que você configurou que o nome pc1.exemplo.com.br corresponde ao endereço 192.168.11.1 (mapeamento direto), mas esqueceu de configurar que o endereço 192.168.11.1 é mapeado no nome pc1.exemplo.com.br. Veja como seria o resultado do `nslookup`:

```
[maria@ns1 ~]$ nslookup
> pc1.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   pc1.exemplo.com.br
Address: 192.168.11.1
> 192.168.11.1
Server:         192.168.1.53
Address:        192.168.1.53#53

** server can't find 1.11.168.192.in-addr.arpa.: NXDOMAIN
```

Sempre que realizarmos uma consulta via `nslookup` e recebermos a resposta "`** server can't find x.: NXDOMAIN`" significa que o servidor não foi capaz de realizar o mapeamento solicitado.

Vamos verificar, com a ferramenta `dig`, se o mapeamento direto e reverso envolvendo pc1 estão casados:

USANDO DIG

```
[maria@ns1 ~]$ dig pc1.exemplo.com.br

; <<>> DiG 9.2.0rc3 <<>> ns1.exemplo.com.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51758
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;pc1.exemplo.com.br.           IN      A

;; ANSWER SECTION:
pc1.exemplo.com.br.    43200   IN      A       192.168.11.1

;; AUTHORITY SECTION:
exemplo.com.br.            43200   IN      NS      ns1.exemplo.com.br.

;; Query time: 2 msec
;; SERVER: 192.168.1.53#53(192.168.1.53)
;; WHEN: Thu Mar 21 19:33:47 2002
;; MSG SIZE  rcvd: 67

[maria@ns1 ~]$ dig –x 150.165.75.21

; <<>> DiG 9.2.0rc3 <<>> -x 192.168.1.53
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;1.11.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
1.11.168.192.in-addr.arpa. 43200 IN    PTR     pc-1.exemplo.com.br.

;; AUTHORITY SECTION:
11.168.192.in-addr.arpa. 43200  IN      NS      ns1.exemplo.com.br.

;; ADDITIONAL SECTION:
ns1.exemplo.com.br.    43200   IN      A       192.168.1.53

;; Query time: 2 msec
;; SERVER: 192.168.1.53#53(192.168.1.53)
;; WHEN: Thu Mar 21 19:31:11 2002
;; MSG SIZE  rcvd: 107
```

Se o status da consulta retornar “NXDOMAIN”, a seção “ANSWER SECTION” não existirá, significando que o mapeamento solicitado não foi possível.

Por fim, vamos realizar nossa verificação de consistência entre mapeamentos direto e reverso correspondentes utilizando a ferramenta `host`:

USANDO HOST

```
[maria@ns1 ~]$ host pc1.exemplo.com.br
pc1.exemplo.com.br has address 192.168.11.1

[maria@ns1 ~]$ host 192.168.11.1
1.11.168.192.in-addr.arpa domain name pointer pc-1.exemplo.com.br.
```

Quando o mapeamento solicitado não for possível a resposta será:

```
[maria@ns1 ~]$ host pc-1.exemplo.com.br
Host pc-1.exemplo.com.br. not found: 3(NXDOMAIN)
```

Uma observação final: nomes de domínio podem ter apelidos. Neste caso, nomes diferentes levarão a um mesmo endereço IP e este endereço IP corresponde a apenas um nome. Quando você solicitar o mapeamento direto de um apelido, o `nslookup`, `dig` e `host` informarão que este nome é um apelido e informa o endereço IP correspondente a este nome de domínio. Não fica caracterizado, portanto, um descasamento de mapeamento direto e indireto. Veja como as ferramentas `nslookup` e `host` informam que ftp é apelido de servidor.exemplo.com.br.

```
[maria@ns1 ~]$ nslookup
> ftp.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

ftp.exemplo.com.br canonical name = servidor.exemplo.com.br.
Name:   servidor.exemplo.com.br
Address: 192.168.1.20

[maria@ns1 ~]$ host ftp.exemplo.com.br
ftp.exemplo.com.br is an alias for servidor.exemplo.com.br.
servidor.exemplo.com.br has address 192.168.1.20
```

Quando for solicitado via `dig` um mapeamento direto de um apelido a seção de resposta virá como exemplificado a seguir:

```
;; ANSWER SECTION:
ftp.exemplo.com.br.        43200   IN     CNAME   servidor.exemplo.com.br.
servidor.exemplo.com.br.    43200   IN      A      192.168.1.20
```

12.6 Consultando o servidor DNS e obtendo respostas com nomes de domínio duplicados

Neste procedimento veremos como realizar diversos tipos de consultas em um servidor de nomes. Veremos como ele responde quando consultamos um nome que envolve o seguinte erro de configuração: ao escrever um arquivo de zona, o administrador da rede usou nomes totalmente qualificados, mas esqueceu de finalizá-los com um "." (ponto).

12.6.1 Descrição e Dicas

Ao escrever um arquivo de zonas, podemos escolher usar nomes relativos ao domínio sendo configurado (www apenas, por exemplo) ou nomes totalmente qualificados (www.exemplo.com.br). Quando usamos nomes completos precisamos terminá-los com um ponto. Um servidor interpreta um nome sem um ponto final como um nome relativo à zona sendo configurada, e acrescenta o nome desta zona a este nome. Consultas a este nome virão com o nome do domínio duplicado. Se o servidor achar o "." após o nome, ele saberá que o nome já está completo e não mais precisará acrescentar a ele o nome do domínio.

12.6.2 Usando nslookup, dig e host

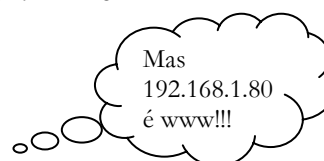
Mostraremos nesta seção como realizar algumas consultas usando `nslookup`, `dig` e `host` que envolvem nomes cuja configuração está levando o servidor a duplicar o nome do domínio.

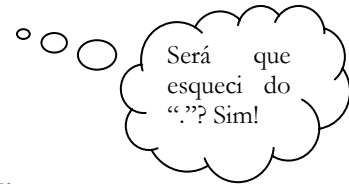
Testaremos a configuração do servidor ns1, do domínio exemplo.com.br. Suponha que o nome da máquina www (192.168.1.80) foi escrito no arquivo de configuração de zona em sua forma completa, mas o administrador da rede esqueceu de pôr o "." final. O mesmo ocorreu com a máquina mail (192.168.1.25) no registro MX e com as máquinas ns2 (192.168.1.54) e ns3 (192.168.1.55) em registros NS. Quando o administrador foi configurar o nome correspondente ao IP 192.168.1.20 no arquivo de configuração de mapeamento reverso (registro PTR), esqueceu de colocar o ponto após o nome completo da máquina ftp.exemplo.com.br. Vamos ver como descobrimos isto realizando algumas consultas.

USANDO NSLOOKUP

```
maria@ns1:~$ nslookup www.exemplp.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

** server can't find www.exemplo.com.br.: NXDOMAIN
> 192.168.1.80
Server:         192.168.1.53
Address:        192.168.1.53#53

80.1.168.192.in-addr.arpa      name = www.exemplo.com.br.
```

Não existe www???

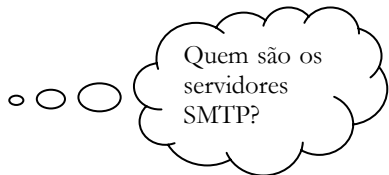
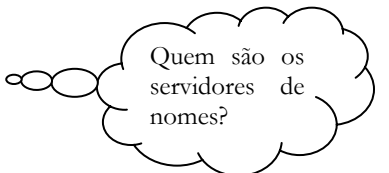
Mas 192.168.1.80 é www!!!

```
> www.exemplo.com.br.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   www.exemplo.com.br.exemplo.com.br.
Address: 192.168.1.80
> ftp.exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

Name:   ftp.exemplo.com.br.
Address: 192.168.1.20
> 192.168.1.20
Server:         192.168.1.53
Address:        192.168.1.53#53

20.1.168.192.in-addr.arpa   name = ftp.exemplo.com.br.1.168.192.in-addr.arpa.
> set type=MX
> exemplo.com.br
Server:         192.168.1.53
Address:        192.168.1.53#53

exemplo.com.br       mail exchanger = 10 mail.exemplo.com.br.exemplo.com.br.
> set type=NS
> pop-pb.rnp.br
Server:         192.168.1.53
Address:        192.168.1.53#53

exemplo.com.br   nameserver = ns1.exemplo.com.br.
exemplo.com.br   nameserver = ns2.exemplo.com.br.exemplo.com.br.
exemplo.com.br   nameserver = ns3.exemplo.com.br.exemplo.com.br.
```

USANDO DIG

As mesmas consultas realizadas com `nslookup` podem ser realizadas com dig. Veja as consultas e algumas respostas:

```
maria@ns1:~$ dig www.exemplo.com.br
; <<>> DiG 9.2.0rc3 <<>> www.exemplo.com.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 32077
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
(…)
maria@ns1:~$ dig –x 192.168.1.80
(…)
;; ANSWER SECTION:
```

```
80.1.168.192.in-addr.arpa. 43200 IN    PTR     www.exemplo.com.br.
(…)
maria@ns1:~$ dig www.exemplo.com.br.exemplo.com.br
(…)
;; QUESTION SECTION:
;www.exemplo.com.br.exemplo.com.br.           IN      A

;; ANSWER SECTION:
www.exemplo.com.br.exemplo.com.br.    43200   IN      A       192.168.1.80
(…)
maria@ns1:~$ dig ftp.exemplo.com.br
(…)
;; QUESTION SECTION:
; ftp.exemplo.com.br.           IN      A

;; ANSWER SECTION:
ftp.exemplo.com.br.    43200   IN      A       192.168.1.20
(…)
maria@ns1:~$ dig –x 192.168.1.20
(…)
;; ANSWER SECTION:
20.1.168.192.in-addr.arpa.  43200  IN  PTR   ftp.exemplo.com.br.1.168.192.in-addr.arpa.
(…)
maria@ns1:~$ dig mx exemplo.com.br
(…)
;; QUESTION SECTION:
; exemplo.com.br.                   IN      MX

;; ANSWER SECTION:
exemplo.com.br.  43200   IN    MX   10 mail.exemplo.com.br. exemplo.com.br.
(…)
maria@ns1:~$ dig ns exemplo.com.br
(…)
;; QUESTION SECTION:
; exemplo.com.br.                   IN      NS

;; ANSWER SECTION:
exemplo.com.br.  86400   IN      NS     ns1.exemplo.com.br.
exemplo.com.br.  86400   IN      NS     ns2.exemplo.com.br.exemplo.com.br.
exemplo.com.br.  86400   IN      NS     ns3.exemplo.com.br.exemplo.com.br.
(…)
```

USANDO HOST

Usando o comando `host`, as pesquisas correspondentes às apresentadas usando `nslookup` e dig são as seguintes:

maria@ns1:~$ host www.exemplo.com.br

```
Host www.exemplo.com.br not found: 3(NXDOMAIN)
maria@ns1:~$ host 192.168.1.80
80.1.168.192.in-addr.arpa domain name pointer www.exemplo.com.br.
maria@ns1:~$ host www.exemplo.com.br.exemplo.com.br
www.exemplo.com.br.exemplo.com.br has address 192.168.1.80
maria@ns1:~$ host ftp.exemplo.com.br
ftp.exemplo.com.br has address 192.168.1.20
maria@ns1:~$ host 192.168.1.20
20.1.168.192.in-addr.arpa domain name pointer ftp.exemplo.com.br.1.168.192.in-addr.arpa
maria@ns1:~$ host -t mx exemplo.com.br
exemplo.com.br mail is handled by 10 mail.exemplo.com.br.exemplo.com.br.
maria@ns1:~$ host -t ns exemplo.com.br
exemplo.com.br name server ns1. exemplo.com.br.
exemplo.com.br name server ns2. exemplo.com.br.exemplo.com.br.
exemplo.com.br name server ns3. exemplo.com.br.exemplo.com.br.
```

Aproveitamos este procedimento para mostrar como realizar tipos diferentes de consultas (NS e MX) no servidor DNS usando `nslookup`, `host` e `dig`.

12.7 Verificando se um servidor SMTP está com repasse totalmente fechado

Neste procedimento mostraremos um teste simples que pode ser realizado para verificar se um servidor de correio eletrônico está negando enviar mensagens para usuários não locais, mesmo quando é um usuário local, usando uma máquina cliente local que solicita o envio da mensagem.

12.7.1 Descrição e Dicas

O servidor de correio eletrônico deve agir de forma seletiva: ele não pode aceitar enviar mensagens de quaisquer remetentes conectados em quaisquer que sejam as máquinas clientes para quaisquer destinatários. Mas ele deve aceitar enviar mensagens solicitadas por usuários conectados em máquinas clientes locais para quaisquer destinatários.

Se um usuário estiver conectado em uma máquina não local e solicitar a entrega de um *e-mail*, o servidor deve aceitar entregá-lo apenas se os destinatários da mensagem forem um ou mais usuários de domínios para os quais o servidor de correio eletrônico está configurado para servir.

12.7.2 Usando uma interface de linha de comando

Nesta seção mostraremos como podemos manipular um servidor SMTP com uma interface de linha de comando e como proceder para testar se um determinado servidor de correio eletrônico está com repasse (*relay*) totalmente fechado.

Conecte-se em uma máquina cliente da rede. Execute nesta máquina o seguinte comando:

```
# telnet IP_do_servidor_SMTP 25
```

Este comando pode ser executado a partir de um *prompt* de comando no Windows. Se você estiver usando um cliente `telnet` Windows, configure-o para realizar eco local do que você digitar. Caso contrário os seus comandos não serão apresentados na tela do `telnet`, pois o servidor de correio não faz *echo* do que recebe do cliente `telnet`.

Após estabelecida a conexão podemos conversar diretamente com o servidor a ser testado.

No exemplo que daremos a seguir estamos testando o servidor mail.exemplo.com.br. Este servidor deve aceitar transmitir mensagens solicitadas por usuários locais conectados em máquinas com IP da rede 192.168.1.0/25.

Efetuamos o *login* na máquina 192.168.1.200 e executamos o `telnet` na porta 25 para servidor de correio eletrônico. Veja como procedemos para testá-lo:

```
# telnet mail.exemplo.com.br 25

220 mail.exemplo.com.br ESMTP

mail from:<maria@exemplo.com.br>

250 ok

rcpt to:<maria@cisco.com>

553 sorry, that domain isn't in my list of allowed rcpthosts
(#5.7.1)

quit

Closing connection. Good bye.
```

Este é um exemplo de mensagem que deveria ter sido aceita para entrega pelo servidor. O remetente é maria@exemplo.com.br, conectada em uma máquina cliente local.

Se o servidor de correio eletrônico estiver corretamente configurado ele aceitará transmitir a mensagem, pois o cliente que solicita o envio da mesma está conectado em uma máquina cliente local:

```
# telnet mail.exemplo.com.br 25

220 mail.exemplo.com.br ESMTP

mail from:<maria@exemplo.com.br>

250 ok

rcpt to:<cris@cisco.com>

250 ok

Data

354 go ahead

teste

.
```

```
250 ok 1018961859 qp 18197
quit
Closing connection. Good bye.
```

12.8 Verificando se um servidor SMTP está com *relay* totalmente aberto

Neste procedimento mostraremos como podemos testar se um servidor de correio eletrônico está aceitando repassar mensagens de qualquer remetente na Internet para qualquer destinatário.

12.8.1 Descrição e Dicas

Um servidor de correio eletrônico com repasse (*relay*) aberto aceita repassar mensagens de quaisquer usuários conectados em quaisquer máquinas no mundo para quaisquer destinatários. Servidores com repasse totalmente aberto são utilizados por *spammers* para enviar mensagens não solicitadas em grande quantidade. Para mais informações veja problema SERVIDOR DE CORREIO ELETRÔNICO COM REPASSE TOTALMENTE ABERTO (página 201).

12.8.2 Usando uma interface de linha de comando

Nesta seção mostraremos um teste simples que pode ser realizado para verificar se um determinado servidor de correio eletrônico está com *relay* aberto.

A interface de linha de comando pode ser obtida através de `telnet`. Conecte-se em uma máquina que certamente não pode ser cliente do servidor SMTP e faça um `telnet` na porta 25 do servidor a ser testado:

```
# telnet IP_do_servidor 25
```

Este comando pode ser executado a partir de um *prompt* de comando no Windows. Se usar cliente `telnet` Windows lembre-se de configurá-lo para realizar eco local dos seus comandos, caso contrário você ao poderá ver o que você digitar.

No exemplo que apresentaremos nesta seção testamos o servidor mail.exemplo.com.br. Este servidor deve aceitar transmitir mensagens solicitadas por usuários locais conectados em máquinas com IP da rede 192.168.1.0/25. Ele considera apenas usuários do domínio exemplo.com.br como usuários locais, isto é, ele não é servidor de correio eletrônico de nenhum outro domínio.

Nos conectamos em uma máquina de uma outra rede cujo IP é 192.168.200.1. A partir desta máquina executamos o `telnet` na porta 25 do servidor de correio eletrônico. Veja a seguir como procedemos para testá-lo:

```
# telnet mail.exemplo.com.br 25
```

```
220 mail.exemplo.com.br ESMTP
helo teste.com.br
250 mail.exemplo.com.br
mail from:<qualquerusuario@qualquerdominio.com.br>
250 ok
rcpt to:<maria@cisco.com>
250 ok
Data
354 go ahead
teste
.
250 ok 1018961859 qp 18197
quit
Closing connection. Good bye.
```

Note que estamos simulando um cliente SMTP na máquina 192.168.200.1, que está solicitando ao servidor de correio eletrônico sob teste que transmita uma mensagem para um usuário que não pertence a nenhum dos domínios que deveriam ser servidos pelo servidor SMTP. Se o servidor de correio eletrônico estivesse corretamente configurado ele só aceitaria transmitir a mensagem se ela estivesse destinada a um usuário do domínio exemplo.com.br.

12.8.3 Usando serviços oferecidos por instituições anti-spam

Nesta seção apresentamos uma outra forma de testar se um servidor de correio eletrônico está com *relay* aberto.

Como apresentado no problema SERVIDOR DE CORREIO ELETRÔNICO COM REPASSE TOTALMENTE ABERTO, existem várias organizações que lutam contra *spammers*. Algumas destas organizações oferecem um serviço que consiste em testar se um determinado servidor de correio eletrônico está inseguro. Em http://www.abuse.net/relay.html e http://mail-abuse.org/tsi/ar-test.html, por exemplo, este serviço é oferecido. Nestas páginas você encontrará a receia completa de como deve proceder para usar o serviço.

12.9 Referências

12.9.1 Livros

[DNS&BIND] 33. Albitz, P. Liu, C. DNS and BIND. Quarta Edição. O'Reilly. Abril, 2001.

ÍNDICE REMISSIVO

A

B

C

D

E

F

G

I

L

M

N

O

P

Q

R

S